携程旅行网文档

携程外部漏洞报告处理流程

< V3.0>

2017 年 7 月

文件修订

版本号	编写人	编写日期	更改内容
v 0.1	CSRC	2014-02	撰写
v 1.0	CSRC	2014-02	修订
v 2.0	CSRC	2016-06	修订
v 3.0	CSRC	2017-07	修订

目录

1、背景

1.1 介绍

携程安全应急响应中心（Ctrip Security Response Center，以下简称为 CSRC，http://sec.ctrip.com）隶属于携程安全中心，是外部用户向携程反馈各业务相关产品安全漏洞的平台，也是携程加强与安全业界同仁的合作交流渠道之一。

1.2 范围

本流程适用于 CSRC 所收到的安全相关的漏洞。

2、基本原则

- 携程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。
- 携程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，帮助携程提升安全质量的用户，我们将给予感谢和回馈。
- 携程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。
- 携程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。
- 携程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。

3、漏洞反馈与处理流程

- **预报告阶段**

漏洞报告者在携程安全应急响应中心（http://sec.ctrip.com）注册帐号。

■ **报告阶段**

漏洞报告者登陆携程安全应急响应中心，提交反馈漏洞（**状态：待审核**）。

■ **处理阶段**

1) 一个工作日内，携程安全应急响应中心工作人员会确认收到漏洞报告并跟进开始评估问题（**状态：审核中**）；

2) 三个工作日内，CSRC 工作人员处理问题、给出结论并计携程币（**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**

业务部门修复漏洞并安排更新上线（**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漏洞 48 小时内，中风险七个工作日内，低风险十四个自然日内。客户端漏洞受版本发布限制，修复时间根据实际情况确定。

■ **完成阶段**

1) 漏洞报告者可以使用已获得积分兑换携程币，并使用携程币在 CSRC 积分商城置换相应礼品，置换完成后，CSRC 为漏洞报告者发出礼品；同时不定期也会有奖励及线下活动。

2) 漏洞报告者同意由 CSRC 不定期挑选有代表意义的漏洞进行分析，分析文章可由 CSRC 免费发表在 CSRC 官网。

4、安全漏洞评分标准

CSRC 采用携程币作为货币单位，1 携程币=1RMB。

■ **Ctrip 应用系统重要性分级标准 ：**

1、核心应用：用户和支付类等基础业务、机票、酒店、旅游、礼品卡、邮轮，评分为：10

2、一般应用：火车票、汽车票、用车、门票、团购、攻略、全球购、商旅　评分：7

3、边缘应用：积分商城、合作卡、订餐、鸿鹄旅游、铁友、艺龙、去哪儿、智行火车票，评分：5

■ **携程币对应表，携程币的=系统重要性*漏洞严重性：**

系统重要性/漏洞严重性	严重漏洞（100-300）	高危漏洞（30-80）	中危漏洞（10-25）	低危漏洞（1-10）
核心应用（10）	1000-3000	300-800	100-250	10-100
一般应用（7）	700-2100	210-560	70-175	7-70
边缘应用（5）	500-1500	150-400	50-125	5-50

■ **漏洞严重性分级：**

【 严重 】

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、缓冲区溢出。

2、直接导致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。

3、严重的敏感信息泄漏。包括但不仅限于核心 DB（资金、用户身份、订单） 的 SQL 注入，可获取大量核心用户的身份信息、订单信息、银行卡信息等接口问题引起的敏感信息泄露。

4、严重的逻辑设计缺陷和流程缺陷。包括但不仅限于通过业务接口批量发送任意伪造消息、任意账号资金消费、批量修改任意帐号密码漏洞。

【 高 】

1、敏感信息泄漏。包括但不仅限于遍历导致大量敏感数据泄露、非核心 DB SQL 注入、源代码压缩包泄漏、硬编码密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。

3、直接获取移动客户端权限。包括但不仅限于远程命令执行、任意代码执行。

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。

【 中 】

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。

2、普通越权操作。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、越权查看用户身份信息等。

3、普通信息泄漏。包括但不仅限于客户端明文存储密码、系统路径遍历。

4、普通的逻辑设计缺陷和流程缺陷。

【 低 】

1、普通 CSRF。

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、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，客户端密码明文传输。

【 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、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。

额外奖励：

1、漏洞影响系统在以上范围之外可计算额外奖励，视具体情况而定。

2、漏洞所涉及系统为核心应用并且漏洞严重等级为严重可计算额外奖励，视具体情况而定，范围在 2000-10000 之间。

■ **评分标准通用原则**

1) 评币标准仅针对携程产品和业务。域名包括但不限于*.ctrip.com，服务器包括携程运营的服务器，产品为携程发布的客户端产品（APP）。与携程完全无关的漏洞，不计币；

2) 现阶段对于非携程直接发布的产品和业务，如携程的投资公司、合资公司、合作区业务，如鸿鹄旅游、艺龙、去哪儿等，不能保证能按照预定时间处理；

3) 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 漏洞等；

4) 同一个漏洞，第一个报告者得币，其他报告者不得币；提交网上已公开的漏洞不计币；

5）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。

6) 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。

5、奖励发放原则

1. 奖品使用携程币（CSRC 漏洞反馈平台上的一种虚拟货币）兑换，携程币数量由 CSRC 评币小组发放，多个漏洞产生的携程币可累加，除非特别声明，未使用的携程币不会过期；

2. 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；

3. 当月兑换的奖品将在第二个月的十五号之前寄出。如因报告者提供错误或未完善资料导致的延误，将在 CSRC 收到正确资料后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延迟送达、丢失或者损坏等，CSRC 不承担责任；

4. 现新增定制礼品页面，如有心仪的礼品，可将需求提交给 CSRC，线下会有专员和您沟通尽可能的满足您的需求。

6、争议解决办法

在漏洞处理过程中，如果报告者对处理流程、漏洞评定、漏洞评分等具有异议的，请在携程安全中心的群里面（qq 号：220392870）及时反馈，会有对应的审核人员给您答疑。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。