完美世界安全应急响应中心

游戏漏洞处理流程与奖励说明 V1.1

完美世界安全应急响应中心

security.wanmei.com

编写人	完美世界安全应急响应中心
版本号	V 1.1
更新时间	2022-03-17

版本号	修订内容	发布日期
V1.0	发布第一版试行	2021-07-26
V1.1	完善评分原则，确定游戏业务范围	2022-03-17

目录

一、 基本原则

1. 完美世界非常重视自身产品和业务的安全问题，我们承诺，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. 完美世界承诺，对于每位恪守“白帽子精神”，保护用户利益，帮助完美世界提升安全质量的白帽子，我们会给予感谢和回馈；
3. 完美世界严禁一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的恶意行为，包括但不限于利用漏洞盗取用户隐私数据及虚拟财产、入侵业务系统、恶意传播漏洞、暗藏木马后门等；
4. 完美世界希望通过此平台与白帽子和安全爱好者建立良好的关系，为完美安全添砖加瓦，为建设安全健康的互联网环境而努力。

二、 适用范围

本流程适用于处理完美世界 SRC 漏洞平台（http://security.wanmei.com）所收到的完美世界所有游戏业务安全漏洞，公司内部人员的漏洞发现除外（内部员工请通过内部 SRC 渠道报告）。

三、 实施日期

本文档自发布之日起实行 。

四、 限制与指引

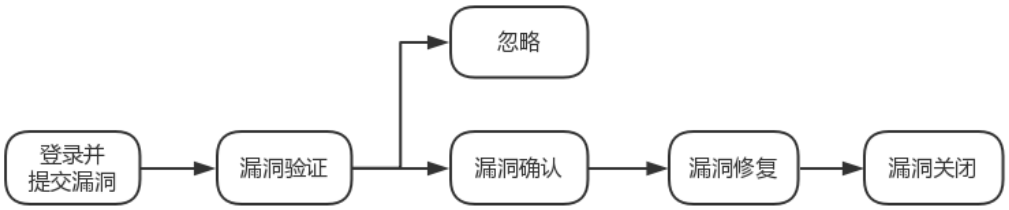
PWSRC 鼓励白帽子积极发现并报告属于完美世界游戏中的安全漏洞，但同时也希望您能遵循以下要求：

1. 测试越权等问题时，请严格限制在测试账号范围内测试，避免影响正常用户；
2. 可能影响其他真实用户的 Payload 请在测试验证漏洞存在后及时删除；
3. 若以上要求确实无法避免的，请及时联系 SRC 运营人员，获得同意后再测试，涉及

到真实账号、用户信息遍历等问题，请严格限制读取条数。

4. 不能破坏游戏的稳定运行，禁止测试任何蠕虫类、拒绝服务类(服务端)漏洞、可能导致拒绝服务的漏洞；客户端拒绝服务漏洞严格控制影响范围；

五、漏洞处理流程



1. 预报告阶段

报告者注册完美通行证账号，并访问 http://security.wanmei.com/（PWSRC 平台）进行登录。

2. 报告阶段

报告者向 PWSRC 提交威胁报告（状态：未处理）

3. 处理阶段

一个工作日内，PWSRC 工作人员会确认收到的报告并跟进评估问题（状态：处理中）。

三个工作日内 PWSRC 工作人员处理问题、给出结论和积分（状态：已确认/忽略）。必要时会与报告者沟通确认，请报告者予以协助。

4. 修复阶段

业务部门修复所报告的问题并安全修复上线（状态：已修复），修复时间根据问题严重程度、修复难度和业务情况而定。一般来说，在漏洞确认后，修复周期为：严重问题不超过 24 小时，高危问题不超过 3 天，中危问题不超过 7 天。如果存在特殊情况，修复时间根据具体情况而定，并与报告者商议修复周期。

5. 完成阶段

<1> PWSRC 完成处理后，更新处理状态，报告者可见更新状态，可以通过积分在 PWSRC 平台兑换礼品。

<2> 对已修复漏洞,报告者可进行复测，若问题仍然存在，可再次报告。PWSRC 工作人员会对该问题进行审查确认，并再次计分或处理。

<3> 对已确认漏洞，3 个月后报告者复测依然存在且 PWSRC 工作人员未与报告者商议修复周期，可再次报告。

六、安全漏洞评分标准

漏洞的最终定级的评价标准在于漏洞对业务本身带来的影响，按照是否核心业务、利用难度、漏洞危害性、影响的用户规模、再现性和是否容易发现等因素，综合评价漏洞对业务的影响。同一漏洞类型，对业务的影响不一致会有不同的漏洞等级。

注：1 积分=5 RMB。具体积分奖励情况请参考下表：

表 6.1 漏洞积分奖励标准

漏洞等级 / 业务等级	严重	高危	中危	低危
核心业务	1000 - 2000	400 - 800	80 - 160	20 - 40
一般业务	600 - 800	200 - 400	40 - 60	5 - 15
边缘业务	120 - 200	60- 80	10 - 20	1 - 5

漏洞等级、业务等级及其定义最终以完美世界审核结果为准

【严重】

1）充值安全漏洞：包括但不限于通过特定手段修改商品价格并能够成功支付，并且虚拟货

币能够到账的漏洞。

2）身份伪造漏洞：包括但不限于伪造系统官方发布官方公告，影响范围较大，造成严重危害的。或者伪造官方向每个玩家发送虚假信息，诈骗信息的漏洞。

3）账号安全漏洞：游戏账号认证方面存在的弱点导致攻击者可以获取大量的用户账号信息，获取到的账号信息可以正常登陆，并能绕过游戏中为敏感行为设置的安全验证机制，如出售、转赠、销毁高价值商品的漏洞。

4）接口安全类漏洞：包括但不限于服务端对客户端的请求未做严格校验措施，导致奖励多次或者无限次数发放，影响到个人游戏数据、破坏游戏运营的。(奖励需有一定的金钱价值)

5）客户端安全漏洞：游戏中使用的第三方组件或者自研组件存在安全漏洞,并且该漏洞可以被远程利用，并且能够达到远程代码执行效果的。

6）其他类型漏洞：任何影响游戏正常营收的漏洞，包括但不限于高价值游戏装备被无限制刷取、游戏装备在交易中存在逻辑缺陷导致游戏营收受影响的漏洞。

【高危】

1）客户端安全漏洞:可远程使客户端无法正常运行、或者使客户端崩溃的漏洞，如未对私发信息进行长度或字符限制导致第三方组件处理接收到的消息时发生崩溃的。

2）影响用户体验、游戏公平性、游戏运营的外挂威胁：包括但不限于飞天、遁地、瞬移、锁血、穿墙、隐身、透视、自动化刷怪等外挂类型，评估标准为外挂需要是定制类型的外挂(使用范围较小)，需要提供相应的外挂样本以及外挂威胁的证据。根据不同游戏类型漏洞等级以最终评级为准。但通过外挂类型只对自身造成影响，并未对其他玩家造成影响的，酌情处理。

3）账号安全漏洞:游戏账号认证方面存在的弱点导致攻击者可以获取大量的用户账号信息，

但获取的账号仅能进行简易的操作、不能实现变卖、转移高价值商品的漏洞。

4）身份伪造漏洞:包括但不限于伪造系统官方发布非官方渠道公告、消息,或者伪装其他玩家和玩家私聊、交易，但未造成严重危害的。

5）设计缺陷漏洞:包括但不限于游戏在玩法上、系统设计，上有缺陷，导致游戏的正常运营、营收、玩家的游戏体验上受到很大影响的。

【中危】

1）设计缺陷漏洞:客户端或服务端逻辑设计缺陷，包括但不限于权限绕过执行未授权行为，如未登陆状态可通过某种手段达到发送信息到公屏的。

2）交互类漏洞:上述高危、严重漏洞中，需要玩家进行交互才可以利用的,包括但不限于访问指定 URL、点击指定按钮的。

3）服务端拒绝服务攻击漏洞:包括但不限于游戏客户端某一接口存在问题导致能高并发请求使服务器无法提供正常服务的漏洞。

4）游戏运营配置漏洞:包括但不限于本地使用某种手段查看购买未上线的活动商品、或者服务端商品未及时下线，导致本地通过某种方式手段能进行成功购买的漏洞。

【低危】

1）拒绝服务漏洞:包括但不限于本地、同局域网、近场通信、第三方组件等其他环境下影响游戏客户端正常运行的漏洞。

2）信息轰炸漏洞:包括但不限于无限制地发送私聊、公屏消息，导致游戏运营的正常消息通知无法正常显示的漏洞。

3）内存修改类漏洞:内存数据修改导致游戏的一些数据属性发生变化从而影响到游戏的正常业务逻辑，但影响范围仅存在于本地的。

4）客户端破解类:修改客户端代码逻辑导致游戏正常业务逻辑受到影响，但影响范围仅限于

本地，并不危及第三方玩家的。

5)敏感词绕过类: 使用某种方式绕过游戏中设置的敏感词体系，评估标准为未绕过前发送失败，绕过后发送成功并能够成功展示的，要求为语意相同，展示效果- -样。包括但不限于游戏昵称、游戏发言。

6 ）其他类型漏洞:如游戏中存在调试页面，通过某种手段打开调试页面，并且调试页面具有非常规功能，导致游戏公平性受到影响的。

【忽略】

1）包括但不仅限于字体乱码，页面显示错乱。

2）使用某种手段绕过客户端的功能逻辑限制的，但没有太大的实际意义的，如绕过强制更新体系。

3）包括但不限于游戏应用中日志开关未关闭，导致调试日志可被查看，但不影响游戏公平性的。

4）以及其他不涉及安全问题的 BUG 等。

七、安全漏洞评分原则

1. 评分标准适用于完美世界的所有游戏产品。包括完美世界各 PC、移动和 web 端的网游等。
2. 游戏业务具体收取范围以完美世界游戏官网为准，官网未上线或者官网已下线的业务，SRC 不予收取。
3. 同一漏洞最早提交者得分，在其它平台上提交过的不计分，与完美世界无关的漏洞不计分。

4、游戏 web 类型的漏洞按照 https://security.wanmei.com/board/detail?id=16 进行处理。

八、奖励兑换

PWSRC 工作人员会在**每个月第一个工作日进行订单确认并进行礼品采购**，首次在平台兑换现金奖励的用户，应公司要求，需要根据平台的引导进行实名认证。如有任何疑问，请联系 src@pwrd.com。奖励的发放需要一定的时间，请各位白帽子耐心等待，感谢理解!

九、争议解决办法

在漏洞报告处理过程中，如果报告者对流程处理、漏洞定级、漏洞评分等有异议的，可以通过 src@pwrd.com 与工作人员及时沟通。

本流程由完美世界集团信息安全部负责修订和解释。