完美世界安全应急响应中心

漏洞反馈处理流程与奖励说明

完美世界安全应急响应中心

security.wanmei.com

版本号	修订内容	发布日期
V1.0	发布第一版	2017-12-20
V1.1	完善评分原则	2018-1-17

目　录

1. 基本原则

1、作为一个负责任的互联网企业，我们深知数据安全的重要性，对于提交有效漏洞的白帽子们，我们将报以由衷的感谢和回馈。我们希望通过此平台与白帽子和安全爱好者建立良好的关系，共同为完美安全添砖加瓦。

2、关于漏洞测试，请以不影响其他正常用户的方式进行。例如在测试越权、XSS 等漏洞时，可注册多个账号进行测试。若无意中改动到了正常用户的信息，请及时告知我们。另外如可能导致系统或业务中断，或可能会造成大面积传播的漏洞不允许进行测试。

3、在已经能够证明漏洞存在的情况下，不允许利用安全漏洞进行破坏、损害用户利益的黑客行为。例如在上传 WebShell 后下载服务器数据，或 SQL 注入时，在已经能够证明 SQL 注入存在的情况下，仍然大量获取用户数据等行为。原则上 SQL 注入时获取的用户数据不要超过 30 组。

4 、对于测试内容，请不要向 PWSRC 之外的任何人或机构提交。一经发现，PWSRC 有权取消奖励并根据具体情节追究相关责任。

2. 适用范围

本流程适用于公司内部及外部人员，但公司内部人员与职务/工作职责相关的漏洞发现除外。

3. 反馈流程

您可以通过 PWSRC 平台（http://security.wanmei.com）直接报告漏洞。
也可将漏洞详情发送至漏洞接收邮箱：src@pwrd.com

4. 安全漏洞评分标准

根据漏洞对公司整体业务的影响程度将漏洞等级分为【严重】、【高危】、【中危】、【低危】、【忽略】五个等级。每种等级认定标准如下：

【严重】
核心应用系统中的高危漏洞，例如：
1、 直接获取核心系统服务器权限的漏洞。包括但不仅限于核心系统服务器的任

意命令执行、上传获取 WebShell、SQL 注入获取系统权限等；
2、 严重的逻辑设计缺陷。包括但不仅限于任意账号登陆、任意账号密码修改、任意账号资金消费；
3、 严重的敏感信息泄露。包括但不仅限于重要数据的 SQL 注入（例如重要的账号密码）、包含敏感信息的源文件压缩包泄露；

【高危】
非核心应用系统中的高危漏洞，例如：
1、 高风险的信息泄露，包括但不限于可以获取一般数据的 SQL 注入漏洞、源代码泄露以及任意文件读取和下载漏洞等；
2、 越权访问，包括但不限于绕过验证直接访问后台、后台登录弱口令、以及其它服务的弱口令等；

【中危】
1、 需交互才能影响用户的漏洞。包括但不限于能够造成切实危害的存储型 XSS；
2、 普通信息泄露。包括但不仅限于获取用户敏感信息、WEB 层的路径遍历等；
3、 普通越权操作。包括但不仅限于越权查看非核心的信息、记录等；
4、 普通逻辑设计缺陷。包括但不仅限于短信验证绕过、邮件验证绕过。

【低危】
1、 有一定价值的轻微信息泄露。比如 phpinfo、测试数据泄露等；
2、 逻辑设计缺陷。包括但不仅限于图形验证码绕过；
3、 有一定轻微影响的 CSRF，反射型 XSS、URL 跳转漏洞等。

【忽略】
1、 不涉及安全问题的 BUG。包括但不仅限于网页乱码、无意义的测试页面等；
2、 其它类型的问题，包含但不仅限于用户名爆破、有条件的 URL 跳转、没有回显且没有内网探测证明的 SSRF、Self-XSS、无敏感操作的 CSRF、无意义的信息泄露、跨域策略文件（crossdomain.xml）、无敏感信息的.htaccess、web.config 文件等。

5. 安全漏洞奖励标准

每个漏洞所得积分=业务等级系数*漏洞积分系数。由完美世界安全应急响应中心结合利用场景中漏洞的严重程度、利用难度、影响范围和提交者关于漏洞描述的详细程度等综合因素进行漏洞评级，并给予相应积分。

注：1 积分=5RMB。具体积分奖励情况请参考下图：

漏洞等级与积分系数 / 业务等级系数	严重（80 - 90）	高危（40 - 45）	中危（10 - 12）	低危（1 - 3）
高（4 - 5）	320 - 450	160 - 225	40 - 60	4 - 15
中（2 - 3）	160 - 270	80 - 135	20 - 36	2 - 9
低 1	80 - 90	40 - 45	10 - 12	1 - 3

6. 安全漏洞评分原则

1、 评分标准适用于完美世界的所有产品和服务。包括完美世界各 PC、移动和 web 端的网游等。
其中核心应用域名如下：
wanmei.com、laohu.com、csgo.com.cn、dota2.com.cn

2、 从 2018 年 1 月 17 日开始，我们将不再接收星游传媒相关域名，包含但不限于：
stargame.com、178.com、tgbus.com、a9vg.com、dospy.com、nga.cn、ngacn.cc、ptbus.com、 766.com、xyous.com 等

3、 针对完美世界使用的第三方系统，或与我们相关的一些边缘业务。我们可能将不完全按照上述评分标准，而是根据业务实际运营情况及所涉及的业务数据进行综合评分。

4、 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。

5、 同一漏洞源引起的多个问题仅记录为 1 个（按引起的最高风险问题计算）。

7. 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。