# 唯品会安全应急响应中心(VSRC)

## ——漏洞处理流程和评分标准 3.3 版

| | |
|---|---|
| 编写人 | 唯品会安全应急响应中心 |
| 版本号 | 3.3 |
| 更新日期 | 2020-3-13 |

# 目录

# 我们承诺

1、 我们承诺，对每一位漏洞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、 唯品会支持合作式的漏洞披露和处理，对于每位恪守白帽子精神，保护用户利益，帮助唯品会提升安全质量的用户，我们将给予感谢和回馈；

3、 唯品会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、 唯品会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“合作式的漏洞披露和处理”过程中来，共建安全健康的互联网环境，共同保护广大互联网用户。

# 一、漏洞反馈和处理流程

## 1.1、预报告阶段

漏洞报告者登陆唯品会安全应急响应中心漏洞反馈平台（http://sec.vip.com/report）注册账号。

## 1.2、报告阶段

漏洞报告者登陆唯品会漏洞反馈平台，提交漏洞信息（状态：未审核）。

## 1.3、处理阶段

三个工作日内，VSRC 工作人员处理问题，给出结论并评分（状态：修复中/已忽略）。必要时会与报告者沟通确认，请报告者予以协助。

## 1.4、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 24 小时内，中风险三个工作日内，低风险七个工作日内。客户端漏洞受版本发布限制，修复时间根据实际情况确定。

## 1.5、完成阶段

VSRC 每季度第一周内，发布上季度的漏洞处理公告，并向上季度的漏洞报告者致谢并发放礼品。

# 二、贡献值和安全币计算方法

1、 【贡献值】由漏洞对应的危害程度以及业务的重要程度决定：

贡献值的计算公式：**贡献值 = 基础贡献值 x 业务系数**

2、 【安全币】由漏洞对应的危害程度以及业务的重要程度决定：

安全币的计算公式：**安全币 = 基础安全币 x 业务系数**

3、 【示例】1 个直接获取核心 WEB 服务器权限的严重漏洞可获得 16,000 元人民币奖励

贡献值 = 基础贡献值（严重：10）x 业务系数（核心：10）= 100 贡献值

安全币 = 基础安全币（严重：60）x 业务系数（核心：10）= 600 安全币

额外奖励 10,000 元人民币 （其余漏洞评分依次类推）

注：“**业务系数**”明细见下文内的第四点

## 2.1、贡献值对应表

| 基础贡献值 / 业务系数 | 严重漏洞（9~10） | 高危漏洞（6~8） | 中危漏洞（3~5） | 低危漏洞（1~2） |
|---|---|---|---|---|
| 核心业务（10） | 90~100 | 60~80 | 30~50 | 10~20 |
| 一般业务（4） | 36~40 | 24~32 | 12~20 | 4~8 |
| 边缘业务（1） | 9~10 | 6~8 | 3~5 | 1~2 |

## 2.2、安全币对应表

| 基础安全币 / 业务系数 | 严重漏洞（55~60） | 高危漏洞（16~20） | 中危漏洞（3~4） | 低危漏洞（1~2） |
|---|---|---|---|---|
| 核心业务（10） | 550~600 | 160~200 | 30~40 | 10~20 |
| 一般业务（4） | 220~240 | 64~80 | 12~16 | 4~8 |
| 边缘业务（1） | 55~60 | 16~20 | 3~4 | 1~2 |

安全币：人民币 = 1:10

# 三、漏洞等级

VSRC 根据漏洞的危害程度将漏洞等级分为【严重】【高危】【中危】【低危】【无影响】五个等级。每个漏洞基础贡献值最高为 10，基础安全币最高为 40。由 VSRC 结合利用场景中漏洞的危害程度、业务的重要程度、利用难度等综合因素给予相应分值和漏洞定级，贡献值将用于礼品奖励发放。每种等级包含的评分标准及漏洞类型明细如下：

## 3.1、严重漏洞

**基础贡献值【9~10】，基础安全币【55~60】**

**额外奖励**

核心业务的严重漏洞达到 100 贡献值，将额外奖励至少 **10,000 元人民币**，且上不封顶

一般/核心业务严重漏洞，会根据实际漏洞情况判定额外奖励

例如： 1 个核心业务严重漏洞 = 业务系数 x 基础安全币 x 人民币比例+额外奖励

= 10 * 60 * 10 + 10,000 = 16,000 元（上不封顶）

严重漏洞等级包括：

1、 直接获取基础架构系统权限包括但不限于：核心业务操作系统、核心业务数据库、防火墙等；

2、 直接获取 Web 服务器权限，包括但不限于：远程命令执行、上传并执行 Webshell、缓冲区域溢出等；

3、 严重的业务逻辑缺陷，可导致：大量用户经济损失，订单及支付系统业务逻辑绕过等；

4、 严重的程序设计缺陷，可导致：大量用户敏感信息泄露，公司内部核心数据泄露等；

5、 可直接导致核心系统瘫痪的拒绝服务攻击漏洞；

## 3.2、高危漏洞

**基础贡献值【6~8】，基础安全币【16~20】**

**额外奖励** 核心业务的高危漏洞最高额外奖励可达 **10000 元**人民币

例如： 1 个核心业务高危漏洞 = 业务系数 x 基础安全币 x 人民币比例+额外奖励

= 10 * 20 * 10 + 10000 = 12000 元

高危漏洞等级包括：

1、 越权访问重要应用系统，包括但不仅限于绕过认证直接访问管理后台，后台系统密码泄露等；

2、 影响一定范围用户账号或资金安全，包括但不限于：非核心 DB SQL 注入，可造成自动传播的存储型 XSS，涉及交易、资金、密码的 CSRF，可导致用户账号安全的应用系统漏洞或业务逻辑缺陷等；

3、 重要业务系统源代码、密钥或未鉴权的 API 的泄露；

4、 公司内部重要数据泄露；

## 3.3、中危漏洞

**基础贡献值【3~5】，基础安全币【3~4】**

例如：1 个核心业务的中危漏洞现金奖励为 400 元

计算方法：核心业务系数 x 基础安全币 x 人民币比例 = 10 * 4 * 10 = 400 元

中危漏洞等级包括：

1、 需用户交互且在主流浏览器中才能产生影响的漏洞，包括但不仅限于针对重要系统的普通存储型 XSS 等；

2、 普通越权操作，包括但不仅限于不正确的直接对象引用，身份数据篡改等；

3、 少量的用户敏感信息泄露，包括但不限于：客户端明文存储密码、个别用户订单或身份信息泄露等；

4、 不涉及资金、订单和用户敏感信息的普通逻辑设计缺陷和业务流程缺陷；

5、 可导致资源滥用或造成对用户骚扰的漏洞，包括但不限于：短信炸弹、邮件炸弹等；

6、 一定量的非重要系统的普通代码泄露；

## 3.4、低危漏洞

**基础贡献值【1~2】，基础安全币【1~2】**

例如：1 个核心业务的低危漏洞现金奖励为 20 元

计算方法：核心业务系数 x 基础安全币 x 人民币比例 = 10 * 2 * 10 = 200 元

低危漏洞等级包括：

1、 只在特定浏览器或客户端环境下才能执行，且影响较小的漏洞，包括但不限于反射型 XSS、非关键业务的存储型 XSS 等；

2、 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 以及非重要敏感操作的 CSRF；

3、 低敏感度信息泄漏，包括但不限于路径泄漏、非核心代码 SVN 文件泄漏、phpinfo 等；

4、 公司内部普通数据泄露，如：内部 IP、系统名称等；

5、 根据设备、系统、软件或框架的官方告警正在修复的漏洞；

## 3.5、无影响

贡献值及安全币均为 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）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)；

3、 无任何证据的猜测；

4、 不可重现且无关紧要的漏洞；

5、 根据设备、系统、软件或框架的官方告警已经修复的漏洞；

## 四、业务系数

VSRC 以业务相关性为依据，将此系数划分为三个等级：核心业务、一般业务、边缘业务

1、 “核心”业务系数为 10，包括：业务中涉及会员、资金、交易、品牌等的核心业务；

2、 “一般”业务系数为 4，包括：业务中不涉及会员、资金、交易、品牌等的一般业务；

3、 “边缘”业务系数为 1，包括：一般业务中的非核心业务，包括由唯品会第三方供应商提供的系统。

## 五、漏洞自动忽略说明

若首次提交漏洞后，审核暂未通过，我们将会以留言或邮件的方式，告知提供更进一步详细说明，待一周后，若白帽子未及时更新补充漏洞说明，则该漏洞将被自动忽略。

# 六、奖励兑换

## 6.1 兑换比例

安全币：人民币 = 1:10

安全币：唯品卡 = 1:10

## 6.2 兑换时间

处理时间：每月的最后一个工作日

最终到账时间：以银行为准

为了保障广大白帽子们的利益，VSRC 会统一将需兑换现金的个人信息，在月底最后一个工作日之前，提交给公司财务，最终金额到账日期，以银行为准，请大家务必耐心等待，感谢理解！

# 七、团队月度奖励细节

| 团队等级 | | 黄金 | 铂金 | 钻石 | 王者 |
|---|---|---|---|---|---|
| 团队因素 | 贡献值 | 大于等于 150 | 大于等于 300 | 大于等于 500 | 大于等于 700 |
| | 人数 | 大于等于 2 | 大于等于 2 | 大于等于 3 | 大于等于 4 |
| | 高危数量 | 大于等于 2 | 大于等于 4 | 大于等于 6 | 大于等于 8 |
| | 严重数量 | 无要求 | 无要求 | 大于等于 1 枚 | 大于等于 2 枚 |
| 现金奖励 | | 4000 元<br>人民币 | 6000 元<br>人民币 | 8000 元<br>人民币 | 1.2 万元<br>人民币 |
| 荣誉奖励 | | 定制奖杯 | 定制奖杯 | 定制奖杯 | 定制奖杯 |

以上数据统计周期为一个月，按照自然月度，以现金奖励形式发放，若当前月度无满足要求上榜安全专家，则奖项自动空缺；

1、获得“黄金”安全团队称号，在当前的评选月度中，至少有 2 名成员出现在月度榜单上，同时团队成员提交的漏洞中至少有 2 个高危漏洞，并且团队在当前的评选月中获得的贡献值至少为 150 分；

2、获得“铂金“安全团队称号，在当前的评选月度中，至少有 2 名成员出现在月度榜单上，同时团队成员提交的漏洞中至少有 4 个高危漏洞，并且团队在当前的评选月中获得的贡献值至少为 300 分；

3、获得“钻石”安全团队称号，在当前的评选月度中，至少有 3 名成员出现在月度榜单上，同时团队成员提交的漏洞中至少有 6 个高危漏洞，其中至少包含 1 个严重级别的漏洞，并且团队在当前的评选月中获得的贡献值至少为 500 分；

4、获得“王者”安全团队称号，在当前的评选月度中，至少有 4 名成员出现在月度榜单上，同时团队成员提交的漏洞中至少有 8 个高危漏洞，其中至少包含 2 个严重级别的漏洞，并且团队在当前的评选月中获得的贡献值至少为 700 分；

5、评选截止时间为每个月的最后一天；

6、 说明：等值面额唯品卡以团队为单位发放；荣誉奖杯以团队为单位发放（即一个团队一个奖杯）；

# 八、个人月度奖励细节

| 安全专家等级 | | V1 | V2 | V3 | V4 |
|---|---|---|---|---|---|
| 个人因素 | 贡献值 | 大于等于 20 | 大于等于 40 | 大于等于 65 | 大于等于 85 |
| | 漏洞要求 | 至少 1 枚中危 | 至少 3 枚中危 | 至少 1 枚高危 | 至少 2 枚高危 |
| | 排名要求 | 至少当月第五 | 至少当月第三 | 至少当月第二 | 当月第一 |
| 现金奖励 | | 1000 元<br>人民币 | 3000 元<br>人民币 | 4000 元<br>人民币 | 5000 元<br>人民币 |
| 荣誉奖励 | | 电子荣誉证书 | 电子荣誉证书 | 电子荣誉证书 | 电子荣誉证书 |

以上数据统计周期为一个月，按照自然月度，以现金奖励形式发放，若当前月度无满足要求上榜安全专家，则奖项自动空缺；

1、获得“V1”级别安全专家称号，在当前的评选月度中，提交的漏洞中至少有 1 个中危漏洞，并且在当前的评选月度中个人获得的贡献值总额至少为 20 分，当月排名≤5；

2、获得“V2”级别安全专家称号，在当前的评选月度中，提交的漏洞中至少有 3 个中危漏洞，并且在当前的评选月度中个人获得的贡献值总额至少为 40 分，当月排名≤3；

3、获得“V3”级别安全专家称号，在当前的评选月度中，提交的漏洞中至少有 1 个高危漏洞，并且在当前的评选月度中个人获得的贡献值总额至少为 65 分，当月排名≤2；

4、获得“V4”级别安全专家称号，在当前的评选月度中，提交的漏洞中至少有 2 个高危漏洞，并且在当前的评选月度中个人获得的贡献值总额至少为 85 分，当月排名第一；

5、评选截止时间为每个月的最后一天；

# 九、 年度奖励细节

1、奖励形式：现金

2、限制条件：（需同时满足）

限制条件 1：仅适用于 VSRC 平台的白帽子

限制条件 2：个人年度贡献值总数需大于等于 100 分

3、年度奖励公布日期：于次年一月份进行核实与结算，并公布年度奖励具体发放日期

4、 年度奖励统计周期：一年一次（即 1 月 1 日至 12 月 31 日）

5、 漏洞基础分：

1 个严重漏洞基础分 **20 分**

1 个高危漏洞基础分 **10 分**

1 个中危漏洞基础分 **1 分**

低危漏洞无基础分

6、 年度奖公式 = 年度贡献值 x（严重漏洞数 x**20** + 高危漏洞数 x**10** + 中危漏洞数 x**1**）

（注意：该基础分，VSRC 会根据当年情况适时做微调）

# 十、季度奖励细节

为鼓励广大白帽提交高质量的有效漏洞信息，每个季度会单独设置特殊奖励，人员数量不限，具体奖励名额根据季度（自然季度）提交漏洞质量而定，**如评估后无符合人员，该奖项则空缺处理**，季度奖励**价值 1000 元——1 万元**的等值礼品奖励或现金奖励。奖励标准如下：

1、提交“严重”级有效漏洞较多的报告者；

2、提交造成较大影响的有效漏洞的报告者；

3、漏洞思路新颖，对唯品会业务安全做出突出贡献的报告者；

4、本季度已获得其余额外奖励，原则不参与季度奖励评选，除特别突出报告者除外。

# 十一、评分标准通用原则

1、 奖励只针对通过 VSRC 平台，唯品会安全应急响应微博，唯品会安全应急邮箱 sec@vipshop.com 提交漏洞的白帽子。

2、 奖励机制只支持唯品会业务，合作方、供应商等第三方公司系统不在此奖励范围内。

3、 同一漏洞产生的多个漏洞，按照最高级别的漏洞奖励标准执行，漏洞数量计为一。例如 PHPwind 的安全漏洞、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、同一个 URL 多个参数的相同问题等。

4、 各等级漏洞的最终积分由漏洞利用难度及影响范围等综合因素决定，若漏洞触发条件非常苛刻，包括但不限于特定浏览器才可触发的 XSS 漏洞，则可跨等级调整积分。

5、 如果同一漏洞或同一问题漏洞的不同表现形式在漏洞修复前由多位漏洞报告者提交，在进行奖励时，我们会以最先提交并清晰表述、重现此漏洞问题的研究者为唯一受奖励者。

6、 漏洞挖掘过程应当以不影响唯品会业务正常运作、不破坏、不传播漏洞为原则，否则唯品会有权取消漏洞奖励。

7、 在漏洞未修复之前，被公开的漏洞不计分。

8、 网上已公开的漏洞不在奖励范围内。

9、 唯品会员工不得参与或通过朋友参与本活动。

10、漏洞奖励处理标准的解释权归唯品会信息安全部门所有。

# 十二、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，可以通过以下三种方式联系 VSRC 工作人员进行及时有效的沟通：

1、 漏洞详情页面的留言板；

2、 邮箱 sec@vipshop.com；

3、 微信公众号“唯品会安全应急响应中心”直接回复留言即可；

VSRC 将按照漏洞报告者利益优先的原则处理，必要时将会引入外部安全人士共同裁定。