唯品会安全应急响应中心(VSRC)

——漏洞处理流程和评分标准 8.1

编写人	**唯品会安全应急响应中心**
版本号	**8.1**
更新日期	**2026-03-12**
修订记录	**V8.1 补充了资产范围，增加了团队奖励说明**

目录

我们承诺

1、 我们承诺，对每一位白帽子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、安全白帽子一起加入到“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；

5、 如果您对本标准有任何建议，欢迎通过 sec@vipshop.com 向我们反馈。

一、漏洞反馈和处理流程

1.1 预报告阶段

白帽子登陆唯品会安全应急响应中心漏洞反馈平台（https://sec.vip.com/report）注册账号。

1.2 报告阶段

白帽子登陆唯品会漏洞反馈平台，提交漏洞信息（状态：未审核）。

报告务必包含「漏洞标题」「漏洞描述」「复现过程」「整改意见」等信息，否则将被做忽略处理。对于将漏洞完整路径、证据截图、危害说明、整改意见描述特别清晰详细的报告，VSRC 将择优对报告者额外奖励并公示，奖励金额以报告实际质量为准，奖励以安全币形式发放至账户。

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，如需补充报告会影响审核时间。

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）。修复时限依据漏洞严重级别及修复复杂度确定，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 次月月初发布上月的漏洞处理公告，向上月的白帽子致谢并发放礼品。

二、业务说明

2.1 业务范围

属于唯品会及旗下的产品和业务，包括但不限于唯品会相关移动应用、客户端、小程序、Web 站点漏洞以及针对唯品会的黑客攻击事件、威胁情报等。

唯品会主要 APP 列举：

唯品会 APP、花海仓 APP、唯享客 APP、唯代购 APP、唯商通 APP

唯品会小程序列举：

唯品会特卖、唯品会折扣店、唯爱妈妈、品生活、塑头古村、花海仓特卖、唯享客、唯品金融、唯品会城市奥莱商户端、唯品会城市奥莱商场端、唯奢品、杉杉奥莱商户管理、杉杉奥莱商场管理、杉杉奥莱、杉杉跨境、小蓉花借钱等。

域名包括但不限于：

.vip.com、.vpal.com、*.vipshop.com、*huahaicang.cn、* shanshan-outlet.com、* shwphxd.com、* loveformum.com。

对唯品会业务无安全风险的报告不计分。

2.2 业务系数

唯品会业务分为三种类型：核心业务、一般业务、边缘业务。

【核心业务】：涉及唯品会主营业务商城的账户、支付、金融、订单详细信息的相关平台或网站，如：唯品会官网、唯品会 APP、唯品会特卖小程序等。

【一般业务】：涉及运营数据、信息统计、公司管理等为公司主营业务提供支撑的系统，如：仓储管理、供应商管理、唯品会开发平台等。

【边缘业务】：唯品会业务相关且非唯品会直接运营的网站/平台，包括但不限于第三方供应商提供的系统，如招聘系统；子公司系统，如：杉杉奥莱系统等。

注：VSRC 会根据应用系统的实际情况动态调整系统的业务系数（如应用系统上线或下线、系统部署环境以及开发人员变化等），并调整制度及公告。

三、漏洞评分标准及奖励

3.1 评分通用原则

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。具体漏洞等级判断由 VSRC 参考下述评分标准，并结合利用场景中漏洞的**危害程度**、**业务重要程度**、**利用难度**等综合因素给予相应分值和漏洞定级。

1、 奖励针对通过 VSRC 平台，唯品会安全应急邮箱 sec@vipshop.com 提交漏洞的报告者；
2、 奖励机制只支持唯品会业务，合作方及第三方公司系统（系统和数据均属于第三方公司）不在此奖励范围内；
3、 同一原因产生的多个漏洞，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白帽子提交，在进行奖励时，我们会以最先提交并清晰表述、重现此漏洞问题的白帽子为唯一受奖励者；

6、 请报告者遵守相关法律规定和《SRC 行业安全测试规范》；

7、 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，请不要在任何情况下泄露漏洞测试过程中所获知的任何信息，未得到 VSRC 允许，请勿对外披露漏洞细节，否则 VSRC 将取消漏洞相关奖励。禁止一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的行为，包括但不限于威胁、恐吓 SRC 要公开漏洞或数据等行为，VSRC 对违法违规者保留采取进一步法律行动的权利；

8、 为针对漏洞进行根因分析，漏洞报告需证明具体漏洞影响，且说明漏洞发现的途径和方法，VSRC 会根据漏洞报告所提供信息完整度及影响综合评定漏洞；

9、 若提交的漏洞不包含于下述常见漏洞类型中，VSRC 将按照漏洞的实际危害性、影响范围、利用难度等进行等级评估；

10、唯品会员工不得直接或通过朋友间接在 VSRC 提交漏洞；

11、漏洞奖励处理标准的解释权归唯品会信息安全部门所有。

3.2 漏洞类型

3.2.1 通用漏洞等级判断

严重漏洞等级包括：

1、 直接获取核心业务和一般业务系统服务器操作系统权限，包括但不限于：远程命令执行、上传并执行 Webshell、缓冲区溢出等；

2、 严重的敏感信息泄漏。包括但不仅限于核心业务系统 DB（资金、用户身份、订单）的 SQL 注入，可获取巨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；

3、 严重的业务逻辑缺陷。包括但不仅限于任意金额支付、无限制大量获取优惠券和津贴、批量修改任意核心系统帐号密码。

高危漏洞等级包括：

1、 直接获取边缘业务系统服务器操作系统权限，包括但不限于：远程命令执行、上传并执行 Webshell、缓冲区溢出等；
2、 直接获取核心系统管理员权限，批量获取一般业务和边缘业务系统权限，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，批量修改任意账号密码；
3、 高风险的敏感信息泄漏漏洞，包括但不仅限于遍历导致大量敏感数据泄露、非核心业务系统 DBSQL 注入、任意文件读取、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，绕过认证直接访问管理后台获取大量敏感信息，利用后台弱密码、SSRF 获取大量内网敏感信息；
4、 越权敏感操作。包括但不仅限于越权修改账号重要信息、进行订单操作、核心业务系统配置修改，大量获取优惠券和津贴操作等。

中危漏洞等级包括：

1、 间接获取核心系统权限和直接获取一般业务和边缘业务系统权限包括但不仅限于存储型 XSS、直接访问管理后台，后台系统密码泄露等；
2、 少量敏感信息泄露，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，越权获取少量用户敏感信息、非核心业务系统的代码泄露等；
3、 普通逻辑设计缺陷，包括但不仅限于越权修改 id、越权修改评论、越权修改订单号、非重要功能接口越权通过并发获取少量优惠券或津贴等；
4、 涉及唯品会账号系统的撞库，爆破等问题。

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、URL 跳转；

3、 低敏感度信息泄漏，包括但不限于路径泄漏、GitHub 泄露的非敏感系统源码及密码、非核心代码 SVN 文件泄漏、phpinfo 等；

4、 无限制短信轰炸漏洞；

5、 根据设备、系统、软件或框架的官方告警正在修复的漏洞；

6、不涉及业务核心功能或非重要敏感信息的增删改查等越权问题。

无影响报告包括：

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)、不可利用的 Self-XSS(无法分享给其他账号访问/未收到后台记录）、静态文件目录遍历、横向短信轰炸、无敏感信息的 log 日志，仅 dns 域名解析记录远程命令执行等；

3、 无法提供完整漏洞证明存在的问题。包括但不仅限于纯属用户猜测、无法重现、未经验证、无意义的扫描报告的问题；

4、 部分风险过低或难以利用的问题。包括不限于 PDF XSS、邮箱轰炸、无法请求内网的 SSRF、并发请求操作某些产品中不重要的数据（如浏览量、报名人数、不重要的点赞评分功能）、无意义的 API Key 泄露、本地拒绝服务漏洞、无意义的源码泄漏、内网 IP 地址/域名泄漏；未提供成功案例，只是说明理论可行（例如只提供 dnslog 的“log4j2 命令执行漏洞”）；

5、 非唯品会业务漏洞、不涉及唯品会产品自身 BUG 且非唯品会产品直接造成的安全问题。

3.2.2 安全情报等级判断

严重漏洞等级包括：

1、核心业务系统、生产及办公网络的入侵情报。如：内网漫游、核心生产服务器入侵、核心数据库的拖库等相关线索；

2、核心业务造成重大影响的威胁情报。如：大规模套现活动、大规模唯品会账号盗取等；

3、大规模敏感信息泄露并验证真实有效的情报。如：会员详细信息、订单详细信息等；

4、重大 0Day 漏洞。如核心服务器软件、系统等未公开或半公开漏洞，核心办公软件等未公开或半公开的漏洞等。

高危漏洞等级包括：

1、非核心业务系统的入侵线索；

2、新型可利用的工具、平台并提供完整可用的工具。如：黑产刷单工具等；

3、造成较大资金损失的威胁情报。例如：有组织的进行薅羊毛行为；

4、金融逻辑漏洞线索。如：支付相关产品的逻辑缺陷，身份信息泄露等。

中危漏洞等级包括：

1、一般风险的业务安全问题。如：优惠券刷取、业务规则绕过、会员权益刷取等；

2、新型可利用的工具、平台。如：扫号工具等；

3、DDOS 情报、攻击时间等相关线索。

低危漏洞等级包括：

1、低风险的业务安全问题。如：批量注册账户等；

2、发现针对唯品会的假冒或者钓鱼网站等。

无效情报包括：

无效威胁情报是指：错误、无意义、与唯品会无关或根据供信息无法调查利用的威胁情报，例如：

1、上报虚假捏造或者无法还原的情报信息；

2、只上报可能套现、刷取利益的聊天群，但未提供其他有效信息；

3、上报已失效的威胁情报。

3.2.3 隐私合规等级判断

接收范围：

1、未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为；

2、非服务所必需或无合理应用场景，特别是在静默状态下或在后台运行时，超范围，超频次收集个人信息的行为；

3、未向用户告知且未经用户同意，私自使用个人信息，将用户个人信息用于其提供服务之外的目的，特别是私自向其他应用或服务器发送、共享用户个人信息的行为；

4、未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为；

5、非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用自动退出或关闭的行为；

6、用户明确拒绝权限申请后，频繁弹窗、反复申请与当前服务场景无关权限的行为；

7、未及时明确告知用户索取权限的目的和用途，提前申请超出其业务功能等权限的行为；

8、未向用户告知且未经用户同意，或无合理的使用场景，频繁自启动或关联启动第三方 APP 的行为；

9、未向用户提供账号注销服务，或为注销服务设置不合理的障碍；

10、使用“偷梁换柱”“移花接木”等方式欺骗误导用户下载 APP，或诱导用户下载非用户所自愿下载 APP 的行为；

11、非服务所必需或无合理场景，通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码以及个人生物特征信息的行为。

严重漏洞等级包括：

1、与相关法律法规存在严重冲突；

2、影响特别严重，涉及核心业务，且严重侵犯用户隐私；

3、发现方式新颖，有一定的技术深度，且对我们后续合规工作用重大帮助。

高危漏洞等级包括：

1、与相关法律法规存在较大冲突；

2、影响严重，涉及核心业务，且侵犯用户隐私或给用户带来较大负面影响。

中危漏洞等级包括：

1、与相关法律法规存在冲突；

2、影响较大，涉及一般业务，且会给用户带来一些负面影响。

低危漏洞等级包括：

1、与相关法律法规存在冲突；

2、影响存在争议或影响相对较小，基本不会给用户带来负面影响。

无效漏洞等级包括：

1、已知或不具实效性的合规风险；

2、不能证实、或没有明确的法律法规依据的合规风险；

3、人为制造的等虚假或无效合规风险。

3.3 数据泄露判断说明

3.3.1 数据范围说明

用户类数据（不限于用户、员工、合作伙伴）：姓名、身份证、手机号、银行卡号、身份证号、住址、邮箱、购买记录、账号密码。（不包含合作伙伴已公开联系方式信息）

3.3.2 数据量说明

数据数量	数量（数据二元组）	数量（数据三元组及以上）
巨量（严重漏洞）	>1000 万条	>100 万条
大量（高危漏洞）	10 万条~1000 万条	1 万条~100 万条
少量（中危漏洞）	1 万条~10 万条	1000 条~1 万条

3.4 漏洞个人奖励

3.4.1 个人贡献值

【贡献值】由漏洞对应的危害程度以及业务的重要程度决定，贡献值高低影响报告者在 VSRC 的排名。

计算公式：贡献值=基础贡献值 x 业务系数

通用漏洞贡献值				
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**

3.4.2 个人安全币奖励

安全币的计算公式：**安全币=漏洞系数 x 业务系数**

漏洞系数 / 业务系数	**严重漏洞 (99-110)**	**高危漏洞 (30-45)**	**中危漏洞 (4-12)**	**低危漏洞 (2-3)**
核心业务（20）	**1980-2200**	**600-900**	**80-240**	**40-60**
一般业务（10）	**990-1100**	**300-450**	**40-120**	**20-30**
边缘业务（1）	**99-110**	**30-45**	**4-12**	**2-3**

3.4.3 额外奖励

1、核心业务的严重漏洞达到 100 贡献值，将额外最高奖励 30 万人民币；

2、一般/核心业务严重漏洞、核心业务的高危漏洞及重大威胁情报，会依据实际漏洞情况判定额外奖励。

3.5 漏洞团队奖励

团队贡献值排行榜， 2026 年起，每季度队当季分数进行排名，对排名前 3 的团队给予现金奖励，给奖励直接给到队长分配；年度给予最终总分排名前五的团队证书和奖杯。每季度积累总排名前三的队长无需安全币，可获得当季活动礼品，例如：给予端午礼盒、中秋礼盒、新年礼盒。

团队人数要求：5=<团队人数=<16

奖励规则：每个季度计算

团队等级	奖励金额	奖励规则
三星攻坚战队	2000 元现金 季度荣誉证书	团队：总贡献值>=50；且提交的有效漏洞>=3 队员：至少 50%以上成员提交过有效漏洞 团队内贡献最多的成员所提交的有效漏洞基础奖励翻倍（当季评定时间内）
四星御守战队	8000 元现金 季度荣誉证书	团队：总贡献值>=200；且提交的有效漏洞>=5 队员：至少 50%以上成员提交过有效漏洞 团队内贡献最多的成员所提交的有效漏洞基础奖励翻倍（当季评定时间内）
五星极客战队	15000 元现金 季度荣誉证书	团队：总贡献值>=500；且提交的有效漏洞>=10 队员：至少 50%以上成员提交过有效漏洞 团队内贡献最多的成员所提交的有效漏洞基础奖励翻倍（当季评定时间内）

说明：奖励由队长领取并负责分配

3.6 漏洞忽略说明

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。

四、平台奖励

4.1 平台奖励兑换

4.1.1 安全币兑换

安全币：人民币=1:10

安全币兑换处理时间：次月月初

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，在次月月初，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！

4.1.2 礼品兑换

VSRC 定期更新商城礼品，每月 15 号左右进行统一邮寄，请及时完善寄送地址，提前兑换礼品。

4.2 特殊奖励

VSRC 以年度贡献值为参考，根据报告者提供有效报告的数量、质量、及沟通与复现效率等综合因素进行评选，对报告者进行年度特别奖励，年度奖励金额最高可达 20 万，具体奖励请关注 VSRC 公告通知。除此之外，VSRC 将不定期推出新人奖励、节日活动、个人/团队奖励等奖励计划，活动发布详情请关注唯品会安全应急响应中心公众号。

五、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，可以通过以下两种方式联系 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；

VSRC 将按照白帽子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。