华住安全响应中心

平台评分和奖励标准 V4.0

编写人	华住安全响应中心
版本号	4.0
更新日期	2022-10-10

版本号	修订内容	发布日期
V3.0	发布评分标准； 发布奖励发放流程。	2019-10-9
V4.0 (试 用 版)	新增隐私类漏洞评分体系与评分规则； 新增【季度】漏洞奖励规则。	2022-08-30
V4.0 (正式版)	更新安全漏洞&安全情报&隐私漏洞评分标准奖励范围； 细化【季度】漏洞奖励规则。	2022-10-10

平台介绍

华住安全响应中心(https://sec.huazhu.com/)是用于提交华住相关漏洞及威胁情报，保障华住用户(以下简称“用户”)信息安全，加强与业界同仁合作、交流的平台。

如果您对本流程有任何建议，欢迎通过邮箱(hsrc@hworld.com)的方式向我们反馈。

适用范围

本规范适用于处理华住安全响应中心平台 (https://sec.huazhu.com)所收到华住相关的安全漏洞及安全情报。

实施日期

本规范自 2019 年 10 月 9 日起正式实施。

一、 基本原则

1) 华住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会有专人进行跟进、分析和处理，并及时给予答复或公告。
2) 我们支持合作式的漏洞披露和处理过程，并承诺对于每位恪守“黑客精神”，保护用户利益，帮助华住提升安全性的安全专家，我们会给予感谢和回馈。
3) 我们严禁一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的黑客行为，包括但不限于利用漏洞入侵业务系统、窃取用户数据、恶意传播漏洞、暗藏木马后门及不完整上报等。
4) 我们认为每个安全漏洞的处理和整个安全行业的进步，都离不开业界各方的共同合作。希望企业、安全公司、安全组织和安全研究者一起加入到“合作式的漏洞披露”过程中来，一起为建设安全健康的互联网环境而努力。

二、 漏洞/情报反馈与处理流程

1) 预报告阶段：漏洞报告者前往华住安全响应中心平台（ https://sec.huazhu.com ）(以下统称“指定平台”)建立账号。
2) 报告阶段：报告者登录指定平台，提交相关信息(状态：漏洞审核中)。
3) 处理阶段：一个工作日内，工作人员会确认收到的报告并跟进开始评估问题(状态：漏洞审核中)，三个工作日内工作人员处理问题、给出结论并计分(状态：已确认/已忽略)。必要时与报告者沟通确认，请报告者予以协助。

4) 修复阶段：针对安全漏洞，业务部门修复漏洞并安排更新上线，修复时间根据问题点严重程度及修复难度而定，一般来说，严重漏洞 24 小时内，高危三个工作日内，中风险七个工作日内。客户端漏洞受版本发布限制，修复时间根据实际情况确定。针对情报，由于情报分析调查的时间较长，因此确认周期相比漏洞的时长较长，具体时间需根据实际情况确定。

5) 完成阶段：完成处理后，更新处理状态，报告者可见更新状态。报告者可通过积分在华住安全响应中心平台兑换礼品。

三、 安全漏洞评分标准

1) 我们支持合作式的漏洞披露和处理过程，并承诺对于每位恪守“黑客精神”，保护用户利益，帮助华住安提升安全质量的安全专家，我们会给予感谢和回馈。

2) 我们严禁一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的黑客行为，包括但不限于利用漏洞入侵业务系统、窃取用户数据、恶意传播漏洞、暗藏木马后门及不完整上报等。

漏洞危害等级 / 影响范围	严重	高危	中危	低危
华住业务	3001-6000 金币	1001-3000 金币	201-1000 金币	1-200 金币

3.1 漏洞危害等级

【严重】

漏洞容易直接或间接利用，利用后会对核心业务/核心服务器、生产环境用户数据造成严重的安全事故。

包括但不限于：

1) 生产业务系统严重的逻辑设计缺陷，包括但不限于账户、支付方面的安全问题，如：任意账户登录、任意账户密码修改、任意账户资金消费、支付交易方面的严重漏洞。
2) 严重的敏感信息泄露，包括但不限于核心 DB(资金、用户、交易相关)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。

【高危】

漏洞一旦被利用会导致业务系统或服务器被直接控制，存在批量数据泄漏、服务器权限被控制等风险。

包括但不限于：

1) 直接获取核心服务器权限的漏洞，包括但不限于任意代码执行、远程命令执行、上传 WebShell 并可执行、SQL 注入获取系统权限、缓冲区溢出(包括可利用的 ActiveX 缓冲区溢出)等。
2) 重要敏感数据信息泄露，包括但不仅限于非核心 DB SQL 注入、源代码压缩包泄漏、服务器应用加密可逆或明文、移动 API 访问摘要、硬编码等问题引起的敏感信息泄露。
3) 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的漏洞。
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) 影响应用正常运转，造成不良影响的漏洞，包括但不限于应用层拒绝服务等。
6) 直接获取非核心业务系统权限的漏洞，包括但不限于可以利用的远程代码执行漏洞等。

【中危】

漏洞被利用后产生的影响在承受的范围内，且不会造成批量数据泄漏，受其他机制有效保护的且较难利用的高危漏洞。

包括但不限于：

1) 普通信息泄露，包括但不仅限于客户端明文存储密码以及 Web 路径遍历、系统路径遍历。
2) 普通越权操作，包括但不仅限于不正确的直接对象引用。

3) 需交互方可对用户产生危害的漏洞，包括但不仅限于一般页面的存储型 XSS、反射型 XSS(包括反射型 DOM-XSS)、重要敏感操作 CSRF。

4) 拒绝服务漏洞。包括但不限于导致网站应用拒绝服务等造成影响的远程拒绝服务漏洞。

5) 本地保存的敏感认证密钥信息泄漏且能做出有效利用。

【低危】

漏洞不会直接造成影响，以普通安全 Bug 的形式存在，漏洞被利用后不会有 用户或服务受到明显的影响。

包括但不限于：

1) 轻微信息泄露，包括但不限于路径信息泄露、SVN 信息泄露、PHPinfo、

2) 异常信息泄漏，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) 本地拒绝服务，包括但不限于客户端本地拒绝服务(解析文件格式、网络协议产生的崩溃)，由 Android 组件权限暴露、普通应用程序权限引起的问题等。

4) 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、可引起传播和利用的 Self-XSS、有一定影响的 CSRF、URL 跳转漏洞。

【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，包括但不仅限于 Self-XSS、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。

四、 安全情报评分标准

威胁系数 / 情报完整性	严重	高危	中危	低危
华住情报	3001-6000 金币	1001-3000 金币	201-1000 金币	1-200 金币

4.1 安全情报威胁系数

【严重】

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。
2) 核心业务造成重大影响的威胁组织活动情报。如：大规模套现活动等。

3) 大规模敏感信息泄露并验证真实有效的情报。如：用户信息、员工信息、订单信息、内部信息等。

4) 本司存在的未公开的 0day 漏洞情报。

【高危】

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) 内部机密泄漏情报。如：尚未公开的活动计划或者方案等。

4) 金融逻辑漏洞线索。如：支付相关产品的逻辑缺陷，加盟商恶意套现牟利手法等。

【中危】

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) 新型的攻击技术或攻击方法。

【低危】

1) 威胁组织基础信息。包括但不限于威胁组织相关人员、架构、规模、地域、活动情况等信息、交流及销售渠道、使用的工具和平台、造成的相关影响、行业动态等。

2) 低风险的业务安全问题。如：批量注册账户等。

4.2 情报完整性说明

由于情报的完整性对情报的价值有着重要的影响，因此上报情报的价值会进行情报完整性考量。情报完整性的评价会综合情报的多个方面进行考虑。华住安全响应中心会根据提供情报的完整度给出 0-10 分的评定，仅上报单一方面的情报将不计分。

情报线索关键点包括：

1) 攻击者个人或者组织的信息，比如身份信息、联系方式、交流渠道等。
2) 攻击者的场景信息，比如产品或业务入口，页面地址等。
3) 攻击过程还原，比如绕过安全校验手法，新型套现的方案或原理等。

【无效情报】 无效威胁情报是指：错误、无意义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) 上报单个或少量酒店的非业务规则问题导致的套现行为。
4) 上报已过期、已失效的威胁情报。

五、 隐私漏洞处理标准

难易程度 / 影响范围	高危	中危	低危
华住业务	1001-3000 金币	201-1000 金币	1-200 金币

5.1 评分说明

1) 仅限于华住会 APP 应用；
2) APP 必须从正规 APP 应用市场或华住官方渠道进行获取，且为该 APP 目前的最新版本；
3) 不包括华住自研应用内所嵌入的由第三方自行收集处理个人信息的页面、SDK 或其他形式的服务，或不面向大众用户提供服务的内部应用或网站；
4) 报告中，需明确 APP 相关版本信息及发布应用市场，并提供隐私风险证明及截图说明，截图包括具体页面、调用栈、接口信息；
5) 测试结果请在第一时间提交 SRC，已经对外公开的合规风险不在收取范围内；
6) 同一 APP，同一类型风险，对于已由其他白帽子或公司内部提前知晓的漏洞，可能会忽略或酌情给予奖励；
7) 未经许可，请不要公开披露或提供关于华住隐私漏洞的任何细节信息或将漏洞提交给第三方，我们保留追回漏洞奖励以及追究法律责任的权利；
8) 相关法律法规参考：

- 工业化和信息化部《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164 号）
- 关于印发《常见类型移动互联网应用程序必要个人信息范围规定》的通知
- 四部委《App 违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191 号）
- 全国信息安全标准化技术委员会《网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南》
- 全国信息安全标准化技术委员会《移动互联网应用程序（APP）系统权限申请使用指南》
- 《中华人民共和国个人信息保护法》
- 《个人信息安全规范》（GB/T 35273-2020）

5.2 难易程度及影响危害

根据隐私漏洞发现的难易程度、影响范围等维度，将隐私漏洞分为高危漏洞、中危漏洞及低危漏洞。

【高危】

1) 漏洞影响重大，与相关法律法规存在较严重冲突，利用方式新颖、有技术深度，未及时修复能够导致公司的经营或声誉等受到严重损害；

2) 问题行业罕见，需要一定的技术深度才能够发现的问题，或针对通用隐私问题可以提供检测脚本。

【中危】

1) 漏洞影响较大，未及时修复可能导致用户投诉、监管机构通报等影响；

2) 一般情况下，该类问题属于监管机构已经明确的检查项目，只需要一般的技术手段就可以发现。

【低危】

1) 漏洞影响小，未及时修复可能产生的影响不明确；

2) 一般情况下，该类问题不需要技术手段就可以发现。

【无】

1) 因“非主流设备不兼容”导致的某些不合规问题不在接收范围内；

2) 未发布上架至各大应用商店，仅在华住相关网站及平台下载的应用，暂不在隐私漏洞收取范围内。

六、 评分标准补充说明

1) 评分标准仅针对在指定平台提交的对华住相关产品和业务有影响的漏洞/安全情报，在漏洞/情报未处理完成前公开的，不计分。

2) 同一漏洞源的多个漏洞，以最高级别的漏洞奖励标准执行，数量记为一个。

3) 以安全测试为借口，利用漏洞进行损害用户利益、影响业务正常运作、私自公开、盗取用户数据等行为的，将不会计分，同时华住安全响应中心将保留采取进一步法律行动的权利。

4) 拒绝无实际危害证明的扫描器结果。

5) 同一漏洞/情报被重复提交的，华住安全响应中心将以最先提交且清晰表达、重现此问题的报告者为唯一奖励者。

6) 各漏洞/情报的最终得分由危害大小、利用难易程度及影响范围综合考虑决定。

7) 由于情报的时效性，报告已知或已失效的情报不计分。

8) 人为自行制造安全威胁或安全事件情报的不计分，同时华住安全响应中心将保留采取进一步法律行动的权利。

七、 个人季度奖励细节

安全等级		L1	L2	L3
影响因素	积分累积	大于等于 20	大于等于 30	大于等于 60
	漏洞要求	至少 3 枚中危或中危级以上	至少 1 枚高危或高危级以上	至少 2 枚高危或高危级以上
	排名要求	至少本季度排行第三	至少本季度排行第二	本季度排行第一
京东卡奖励		**2000 元**	**4000 元**	**6000 元**
荣誉奖励		电子荣誉证书	电子荣誉证书	电子荣誉证书

以上数据统计按照自然季度，以京东卡奖励形式发放，若本季度无满足要求上榜的人员，则奖项自动空缺，若有相同分数并列排名产生，按照提交漏洞时间排名前后，2 人以内的人员均按照相应标准发放等级奖励，之后的人员排名顺移；

1、获得“L1”级别安全专家称号，在当前的评选季度中，提交的漏洞中至少有 3 个中危或中危级以上漏洞，并且在当前的评选季度中个人获得的排行榜积分

总额至少为 20 分，当前的评选季度中排名≤3；

2、获得“L2”级别高级安全专家称号，在当前的评选季度中，提交的漏洞中至少有 1 个高危或高危级以上漏洞，并且在当前的评选季度中个人获得的排行榜积分总额至少为 30 分，当前的评选季度中排名≤2；

3、获得“L3”级别资深安全专家称号，在当前的评选季度中，提交的漏洞中至少有 2 个高危或高危级以上漏洞，并且在当前的评选季度中个人获得的排行榜积分总额至少为 60 分，当前的评选季度中排名第一；

4、评选截止时间为每个自然季度的最后一天。

八、 奖励发放原则

常规奖励：奖品使用金币兑换，1 金币=1RMB。积分数量由漏洞/情报的评分乘以相应的危害系数计算得出。积分不会过期。现金礼品将于次月月中完成打款，非现金礼品于每月月底统一寄送，如兑换者未能及时完善个人信息导致礼品不能按时发放的，将顺延至下月发放；如因礼品兑换者个人过失、快递公司问题及人力不可抗拒因素导致的奖品损坏及/或丢失，华住安全响应中心不承担责任。

特殊奖励：华住安全响应中心将不定期举行特殊活动，发放对应活动奖励。对于价值较高的漏洞/情报，我们将发放额外奖励。 具体发放规则将在活动前以公众号文章形式发布，奖励标准及礼品管理以活动公告为准。

特别提醒：对于华住员工，请至内部平台提交漏洞。提交自己所负责业务的安全漏洞不予奖励。

九、 争议解决办法

在漏洞/情报处理过程中，如果报告者对处理流程、评分等有异议的，可通过以下方式联系华住安全响应中心工作人员：

（1）华住安全响应中心(https://security.huazhu.com)平台安全报告的详情页留言板留言。

（2）邮箱地址：hsrc@hworld.com。

华住安全响应中心将按照报告者利益优先的原则处理，必要时会引入外部安全人士共同裁定。