小米安全中心
Xiaomi Security Center

隐私漏洞奖励判定规则v3.1

版本号	修订内容	发布日期
V3.1	新增隐私漏洞报告要求； 完善漏洞奖励定级； 完善漏洞接受范围；	2022-7
V3.0	隐私漏洞评分细则	2022-2
V2.0	隐私漏洞奖励全面升级； 新增隐私漏洞月度季度奖励；	2021-11
V1.0	发布第一版	2020-1

一、 基本原则

小米安全中心紧跟法律法规要求，希望通过隐私众测培养一批隐私蓝色军团，提升内部合规能力。我们承诺：每一份报告我们都会有专人进行评估和跟进，会向隐私漏洞的提供者给予匹配奖励。

小米反对和谴责损害公司利益的行为，未经允许请勿在任何公众场合或平台讨论或披露隐私漏洞的细节，不得向任何第三方透露隐私漏洞。如有上述行为，小米将有权追究其法律责任。

二、 争议及解决方法

1.一般情况下，按奖励评级细则进行分级奖励；

2.针对有争议的问题，将在安全团队组内讨论后，进行投票评级；

3.安全团队对评级细则拥有最后的解释权。

三、 漏洞特色奖励

月度额外奖励（和安全漏洞一起评判）

- 奖励金额：第一名额外奖励￥2000、第二名奖励￥1500、第三名额外奖励￥1000
- 参选条件：当月贡献值超过600分且贡献榜排名前5名
- 规则说明：如在当月度结束后未有达到规则的安全专家，奖励名额将作废

季度额外奖励

等级	隐私漏洞	额外奖励
LV2	贡献值≥2000	Y*80贡献币+￥3000
LV1	贡献值≥1000	Y*60贡献币+￥2000
Y=【中危漏洞数】/10+【高危漏洞数量】		

四、 隐私漏洞评分细则

业务范围：所有面向终端用户的小米应用

根据隐私问题发现的难易程度、影响发小、发生可能性等维度，将隐私漏洞分为高危漏洞、中危漏洞及低危漏洞。

对于涉及影响巨大且对小米安全有特殊帮助的漏洞/情报，经小米安全中心核验后，将额外再给予2k-2w的额外奖励。

非小米资产：米筹、小米彩票、智米、黑鲨、省钱购、米灵、小蚁、小米运动（华米-生态链）**注：该内容会随业务实际情况不断更新，敬请关注**

对于同一问题在多个App中发现的情况，建议合并提交一个漏洞，我们会根据漏洞具体情况给予双倍奖励，并给予额外奖励。

漏洞级别	判定标准： 与主要用户所在的国家或地区的相关法律法规冲突，未及时修复能够导致企业的经营、或声誉等受到损害；	奖励标准（贡献币）
高危	直问题新颖且行业内罕见，需要一定技术深度才能够发现的问题	300-500
中危	一般情况下，隐私漏洞的发现与鉴别需要一定的技术手段。包括但不限于： 1 同意隐私政策前收集个人信息或打开个人信息权限； 2 强制定向推送信息； 3 若通过嵌入第三方代码插件收集个人信息的功能，是否向用户明示； 4 调用与服务或功能无关的权限； 5 除此之外，隐私政策中的重要内容遗漏，也属于中危险漏洞，包括： 6 收集个人信息的范围超出隐私政策中描述的范围； 7 收集的频率超出其实现产品或服务的业务功能所必需的最低频率。	80-120
低危	违反下一般情况下，该类问题不需要技术手段就可以发现，如隐私政策中描述性内容文本遗漏等，包括但不限于： 1 未告知个人信息处理者的名称或者姓名和联系方式； 2 未告知个人信息的处理目的、处理方式，处理的个人信息种类、保存期限； 3 未告知个人行使本法规定权利的方式和程序，例如复制、删除或更正个人信息的途径； 4 隐私政策的文本不易于阅读，例如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等；	10-30

漏洞忽略：

一般情况下，该类问题判断所依据的法律、法规和标准中的相关要求处于暂未发布施行的状态（如草稿、征求意见稿、未实施），或已发布但只面向部分行业生效或暂未实质推行（如面向部分行业的推荐性标准只针对对应行业生效），隐私政策中错别字问题（持续更新）；

隐私漏洞报告要求：

技术类隐私漏洞需提供有效的日志类信息，包括但不限于：完整的测试堆栈信息、其网络流量抓包截图、284log或其他日志文件。只提交检测平台、检测工具类的结果截图类证据将不被接受。

仅以静态扫描Manifest结果为依据提交的缺少相关隐私声明的漏洞，但没有提供实际调用记录的，确认为低危，有调用记录的，确认为中危。

仅提供SDK列表截图，白帽子提示SDK列表不全以外，还应当补充提交关于SDK实际传输了数据给第三方的证据。否则不予通过。

提交MIUI默认安装的系统应用相关隐私漏洞时，请确认此隐私漏洞发现于最新稳定版MIUI系统。

漏洞接收范围：

七大类漏洞类型	
隐私声明存在缺陷	1. 收集用户数据，但无隐私政策 2. 存在数据共享，但无第三方数据共享清单 3. 首次打开APP无隐私政策弹窗 4. 隐私政策中内容缺失（如缺少字段或权限声明） 5. 隐私政策需4步以上才能访问 6. 敏感个人信息未加粗展示 7. 第三方数据共享内容缺失
不合规数据采集	1. 隐私政策同意前上传个人信息 2. 未经授权采集或上传个人信息 3. 频繁采集用户个人信息 4. 收集与服务或功能无关的数据
不合规隐私权限使用	1. 未经授权调用个人信息权限 2. 权限使用前未同步告知使用目的 3. 频繁调用个人信息权限

	4. 调用与服务或功能无关的权限 5. 用户拒绝后频繁询问用户授权
用户权利问题	1. 未按法律规定提供复制、删除或更正个人信息途径 2. 缺少注销、撤回同意等功能 3. 缺少个性化广告或个性化推荐开关
产品设计缺陷	1. 隐私政策存在默认同意 2. 隐私政策勾选按钮无法点击 3. 隐私相关的产品功能无法使用或不生效 4. 授权过程或同意过程可绕过 5. 授权或同意界面反复弹出
其他	

参考标准

- 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）
- 常见类型移动互联网应用程序必要个人信息范围规定
- 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）
- 《中华人民共和国个人信息保护法》
- 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求
- 网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南