百度安全应急响应中心隐私漏洞处理标准 1.0

一、 基本原则

百度密切跟进和遵从监管合规和法律法规要求，通过百度安全应急响应中心（简称 BSRC）收录隐私合规漏洞致力于更好守护百度移动产品隐私安全性，以此不断提升百度内部相关能力。本则标准描述了 BSRC 处理隐私漏洞报告时的具体流程和做法，同时公示了对于不同等级漏洞的奖励标准，为漏洞发现者及漏洞报告者从事漏洞发现和报告的活动提供指引。

针对提交的隐规漏洞，会有内部安全合规专家进行评审和跟进，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，百度将有权追究其法律责任。

二、适用范围

百度 APP、百度地图、百度极速版、百度网盘、好看视频、百度输入法、百度贴吧、百度翻译、百度手机助手、萝卜快跑、百度 Carlife+、小度

三、限制与指引

- 来源合规性：APP 必须从正规 APP 应用市场或百度官方渠道获取，且为当时该 APP 的最新版本。补充说明：
  - 若同一产品在各应用市场版本不一致，则以最新版本号为准；
  - 若在 BSRC 正式提交漏洞报告前，此窗口期内 APP 更新了版本，则应以新发布版本为准。
- 名词标准化：隐私风险中名词的定义和内容参考 GB/T 35273-2020《信息安全技术个人信息安全规范》；

- 信息完整性：提交漏洞报告时，需提供完整检测信息，包括：名称、APP 来源、版本号、测试工具、复现路径、隐私风险证明及清晰截图证据，其中截图证据必须至少包括问题所在界面、接口、调用栈；
    - 说明：对于无需技术手段即可发现的风险（如：信息窗口未提供显著的关闭或退出选项）可不提供接口、调用栈信息
- 及时度要求：测试结果请在第一时间提交至 BSRC，已经对外公开的隐私漏洞不在收取范围内；
- 计分规则：
    - 相同类型隐私漏洞在同一 APP 中发现的，按照一个漏洞评定和给予奖励；
    - 相同类型隐私漏洞在同一 APP 中发现的，第一个报告者获得奖励，后续报告者不再奖励；
    - 相同类型隐私漏洞在多个 APP 中发现的，请合并一个漏洞报告提交，我们会根据漏洞具体情况给予额外奖励；
    - 对于公司内部提前知晓的隐私漏洞，可能会忽略或酌情给予奖励；

四、漏洞评分细则

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

漏洞级别	判定标准	奖励标准（安全币）
高危	问题新颖且行业内罕见，漏洞的发现与鉴别需要一定的技术手段，或涉及用户范围较大、对用户权益影响较大	400-800

中危	漏洞的发现与鉴别无需技术或者简单技术即可以发现，或涉及用户范围较小、对用户权益影响较小。 包括但不限于： ● 同意隐私政策前收集个人信息或打开个人信息权限 ● 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 ● 收集的个人信息范围超出了隐私政策中描述的范围 ● 未经用户同意，非服务所必需或无合理场景，APP 切换至后台后持续收集个人信息 ● 无隐私政策或隐私政策难以访问(如进入 APP 主界面，需多于 4 次点击等才能访问到)	80-120
低危	漏洞的发现与鉴别无需技术或者简单技术即可以发现，或涉及用户范围较小、对用户权益影响较小。 包括但不限于： ● 隐私政策未见向用户明示、未经用户同意，存在采集个人信息行为。 ● 既未经用户同意，也未做匿名化处理，App 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方	10-30

	提供个人信息 ● 非服务所必须或无合理需求，提前向用户申请权限 ● 欺骗强迫用户下载且无法关闭或停止 ● APP 频繁索权，用户拒绝权限申请后，在非用户主动触发权限所涉及的业务场景的情况下，再次弹出权限弹窗即为频繁 说明：仅以静态扫描 Manifest.xml 结果作为缺少隐私声明依据，但没有提供 APP 实际调用记录的漏洞，认定为无效漏洞	

五、报告提交要求

漏洞报告者可以通过 BSRC 平台（https://bsrc.baidu.com）注册并提交漏洞。

提交报告时，请在漏洞类型处勾选【隐私安全漏洞】，且需要提供以下关键信息：

- 基本信息字段：APP 产品名称、APP 产品版本（必须为最新版本）、APP 下载来源、APP 安装文件、测试方式（工具名称和测试方法）、复现路径、整改建议等；
  - 若同一产品在各应用市场版本不一致的，则以最新版本号为准；
  - 若在 BSRC 正式提交漏洞报告前，此窗口期内 APP 更新了版本，则应以新发布版本为准。
- 隐私漏洞证明：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。

六、补充说明及注意事项

以下情况将不计入有效漏洞：

- 在漏洞修复之前被公开的漏洞；
- 网上已公开的漏洞；
- 以测试漏洞为理由，利用漏洞进行损害用户利益、影响业务运作、盗取用户数据等行为的，将不被计入，同时百度保留采取进一步法律行动的权利；

以下情况将做降级/追回奖励处理：

- 对于缺乏关键因素（文字描述、测试过程、风险接口和参数等），报告排版混乱，无法稳定复现的报告，将做降级/忽略处理；
- 未经百度许可，私自对外透漏漏洞详情，追回漏洞奖励且保留法律起诉的权利；
- 对于同一个 URL，如果多个参数存在类似的漏洞，按一个漏洞积分，不同类型的，按危害程度最大的计分；
- 同一个漏洞源产生的多个漏洞计算为一个漏洞。
- 提交漏洞时请确认是否会对业务有真正的影响，并提交实际产生危害的证明，对于间接危害或猜测危害，定级时将不予考虑。

附：法规标准

- 《App 违法违规收集使用个人信息行为认定方法》
- 《工业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》
- 《常见类型移动互联网应用程序必要个人信息范围规定》
- 《中华人民共和国个人信息保护法》
- 《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》

2023 年 7 月