南明离火
移动应用检测平台

ANDROID 静态分析报告

大转盘小决定 • v2.1.1

分析日期: 2024-06-17 10:07:09

应用概览

文件名称:	com.leandom.dice_2.1.1.apk
文件大小:	16.47MB
应用名称:	大转盘小决定
软件包名:	com.leandom.dice
主活动:	com.leandom.dice.activity.SplashActivity
版本号:	2.1.1
最小SDK:	21
目标SDK:	33
加固信息:	360加固 加固
应用程序安全分数:	41/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估：安全
MD5:	8b929595b25c3dee88f67edf5383de78
SHA1:	caf442540d37c3e6e820a6b309e7cde652c48e84
SHA256:	e0042c8872d097a775c7ed5f23b5600fda828517ff9b05e8ba944ed476a481e9

分析结果严重性分布

高危	中危	信息	安全	关注
2	10	2	0	8

四大组件导出状态统计

Activity组件：67个，其中export的有：0个
Service组件：8个，其中export的有：1个
Receiver组件：1个，其中export的有：0个
Provider组件：0个，其中export的有：0个

应用签名证书信息

二进制文件已签名

v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=cn, ST=Fujian, L=Xiamen, O=leandom, OU=leandom, CN=leandom
签名算法: rsassa_pkcs1v15
有效期自: 2018-03-17 03:42:30+00:00
有效期至: 2043-03-11 03:42:30+00:00
发行人: C=cn, ST=Fujian, L=Xiamen, O=leandom, OU=leandom, CN=leandom
序列号: 0x25cddf27
哈希算法: sha256
证书MD5: 5ae820dd6dc38e33ab664e42350f6bf8
证书SHA1: b81c8394e19a4d67cfe4440953ede234949e4f94
证书SHA256: eef1a35d52fbd69a5146ed0fc879f328d31ccee0b6c9edecc3b318928de7c25c
证书SHA512:
77346a09124c659f50e7f477c0f196356eb820ae3d610e64c75c55a3207e1cd7d95befe1096265e8a9f668e88343a2e3040a171e93a1915b82a2d2fea0a5f322

公钥算法: rsa
密钥长度: 2048
指纹: 0a353692525379d7276155c637f0c9bb995dc90dfb6fc51aa6c8f482842270d1
找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
com.leandom.dice.openadsdk.permission.TT_PANGOLIN	未知	未知权限	来自 android 引用的未知权限。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名

Manifest 配置安全分析

高危: **0** | 警告: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup] 应该设置为false。默认情况下它被设置为true，允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
3	Service (com.ss.android.socialbase.downloader.downloader.IndependentProcessDownloadService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问，intent-filter的存在表明这个Service是显式导出的。

代码安全漏洞检测

高危: **2** | 警告: **7** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

3	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
4	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
5	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
6	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
7	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
8	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
9	应用程序使用SQLite数据库执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
10	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限

11	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE com.google.android.gms.permission.AD_ID android.permission.CHANGE_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.REORDER_TASKS

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息
www.chengzijianzhan.com	安全	是	**IP地址:** 121.228.130.192 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
apps.bytedance.com	安全	是	**IP地址:** 121.228.130.192 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
i.snssdk.com	安全	是	**IP地址:** 121.228.130.192 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图

sf6-ttcdn-tos.pstatp.com	安全	是	**IP地址:** 121.228.130.192 **国家:** 中国 **地区:** 浙江 **城市:** 台州 **纬度:** 28.666668 **经度:** 121.349998 **查看:** 高德地图
www.toutiaopage.com	安全	是	**IP地址:** 121.228.130.192 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
apps.bytesfield-b.com	安全	是	**IP地址:** 59.222.17.207 **国家:** 中国 **地区:** 江苏 **城市:** 宿州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
paixiangxian.com	安全	是	**IP地址:** 121.228.130.192 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
apps.oceanengine.com	安全	是	**IP地址:** 121.228.130.192 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
www.samsungapps.com	安全	否	**IP地址:** 52.31.24.56 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图

URL链接安全分析

URL信息	源码文件
• https://www.samsungapps.com/appquery/appdetail.as?appid=	com/ss/android/downloadlib/a/xl.java
• http://paixiangxian.com/xiaojueding/agreement.html • http://paixiangxian.com/xiaojueding/privacy.html	com/leandom/dice/activity/SettingActivity.java
• https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java

• https://apps.bytesfield-b.com • https://apps.bytesfield.com	com/ss/android/downloadlib/addownload/compliance/c.java
• https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
• www.chengzijianzhan.com • https://apps.oceanengine.com/customer/api/app/pkg_info? • www.toutiaopage.com/tetris/page	com/ss/android/downloadlib/addownload/compliance/bk.java
• http://paixiangxian.com/xiaojueding/agreement.html • http://paixiangxian.com/xiaojueding/privacy.html	x0/b.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Pangle SDK	ByteDance	穿山甲是巨量引擎旗下全球应用变现与增长平台，汇聚优质媒体超 30,000 家，日请求突破 607 亿，日均展示达 100 亿，覆盖 7 亿日活用户，为全球应用和广告主提供高效的用户增长和变现解决方案。
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品，在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
腾讯广告 SDK	Tencent	腾讯广告汇聚腾讯公司全量的应用场景，拥有核心行业数据、营销技术与专业服务能力。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

邮箱地址敏感信息提取

EMAIL	源码文件
leandom@163.com	p0/v.java

第三方追踪器检测

名称	类别	网址
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
AYoGreCptsEmQzlnkg2H51UTKpYl3poR

免责声明及风险提示: