南明离火
移动应用检测平台

ANDROID 静态分析报告

sollys • v0.1

分析日期: 2025-04-04 04:58:43

应用概览

文件名称:	sollys v0.1.apk
文件大小:	4.01MB
应用名称:	sollys
软件包名:	com.wsollys
主活动:	.MainNavigationActivity
版本号:	0.1
最小SDK:	23
目标SDK:	23
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	40/100 (中风险)
跟踪器检测:	7/432
杀软检测:	12 个杀毒软件报毒
MD5:	3dab3b0ec6dd62f191d45e779d347f23
SHA1:	35dc1647820b962dd2bf331484b23e4bd7677876
SHA256:	41a66f1f4f78e813f473c55976b4c0b3ef57b37f2694f997f29666f30b231235

分析结果严重性分布

高危	中危	信息	安全	关注
6	17	1	1	0

四大组件导出状态统计

Activity组件：20个，其中export的有： 0个
Service组件：5个，其中export的有： 0个
Receiver组件：6个，其中export的有： 5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: False
v3 签名: False
v4 签名: False
主题: C=CHINA, ST=HUBEI, L=WUHAN, O=HUST, OU=BIAC, CN=oscar
签名算法: rsassa_pkcs1v15
有效期自: 2023-09-21 08:30:17+00:00
有效期至: 2123-08-28 08:30:17+00:00
发行人: C=CHINA, ST=HUBEI, L=WUHAN, O=HUST, OU=BIAC, CN=oscar
序列号: 0x7591f516
哈希算法: sha256
证书MD5: 4fcb5f606276cfd3121c527f89e7b995
证书SHA1: 2ef4a2c0e48fcf9c06b760340531dfef5ea2cf1c
证书SHA256: 07e9d6a57f5a869903ce235cc98639525ef7f12e9e4b87e7da74c6c31ecaacdd
证书SHA512:
e8d7ce00a9cc85d98b0aabda06edd5510a6fbb4f2306828812ae9f8217c3fba54d4fea40c90510aacd25e64a9a6557e8ac9b096f7230629a2565e411ca7fa955

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.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.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
com.wsollys.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
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.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。

可浏览 Activity 组件分析

ACTIVITY	INTENT
.MainNavigationActivity	Schemes: http://, https://,

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: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名
应用程序容易受到 Janus 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-7.0 上容易受到 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

Manifest 配置安全分析

高危: **2** | 警告: **6** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
2	Activity （.MainNavigationActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
3	Activity （com.wsollys.VideoPlayerActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
4	Broadcast Receiver (com.google.android.gcm.GCMBroadcastReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
5	Broadcast Receiver (.pull.PullServerController) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
6	Broadcast Receiver (com.wsollys.server.CampaignReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Broadcast Receiver (com.inmobi.commons.core.utilities.uid.ImIdShareBroadCastReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

本报告由南明离火移动安全分析平台生成

8	Broadcast Receiver (.notification.NotificationCheckerBootReciever) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。

代码安全漏洞检测

高危: **2** | 警告: **10** | 信息: **1** | 安全: **1** | 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	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
3	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
4	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
5	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
6	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

8	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
9	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
10	应用程序使用SQLite数据库并执行原始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
11	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
12	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
13	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息。	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
14	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限

00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限

00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	升级会员：解锁高级权限
00204	获取默认铃声	信息收集	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00064	监控来电状态	控制	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	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	4/30	android.permission.READ_PHONE_STATE android.permission.SYSTEM_ALERT_WINDOW android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	4/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE android.permission.WRITE_EXTERNAL_STORAGE

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
updapp.com	安全	否	**IP地址:** 107.20.182.195 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
d1byvlfiet2h9q.cloudfront.net	安全	否	**IP地址:** 34.110.179.88 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
tm.inmobi.com	安全	否	No Geolocation information available.
inmobisdk-a.akamaihd.net	安全	否	**IP地址:** 129.213.103.0 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
iccto.net	安全	否	**IP地址:** 107.20.182.195 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
init.startappexchange.com	安全	否	**IP地址:** 129.213.103.0 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
silvermob.com	安全	否	**IP地址:** 173.208.1.21 **国家:** 美国 **地区:** 伊利诺伊州 **城市:** 芝加哥 **纬度:** 41.875771 **经度:** -87.620605 **查看:** Google 地图
a.applovin.com	安全	否	**IP地址:** 129.213.103.0 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

live.chartboost.com	安全	否	**IP地址:** 34.107.157.36 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
d.applovin.com	安全	否	**IP地址:** 34.110.179.88 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
splash.appsgeyser.com	安全	否	**IP地址:** 142.250.189.14 **国家:** 美国 **地区:** 哥伦比亚特区 **城市:** 华盛顿 **纬度:** 38.895390 **经度:** -77.039474 **查看:** Google 地图
www.startappexchange.com	安全	否	**IP地址:** 129.213.103.0 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
www.dummy.com	安全	否	**IP地址:** 129.213.103.0 **国家:** 美国 **地区:** 佛罗里达州 **城市:** 坦帕 **纬度:** 27.943518 **经度:** -82.510269 **查看:** Google 地图
config.inmobi.com	安全	否	**IP地址:** 34.117.147.68 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
market.android.com	安全	否	**IP地址:** 142.250.189.14 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
app2ad.com	安全	否	**IP地址:** 107.20.173.57 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图

androidads23.adcolony.com	安全	否	**IP地址:** 35.186.210.75 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
iccto.com	安全	否	**IP地址:** 107.20.182.195 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 172.66.0.227 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
stat.appsgeyser.com	安全	否	**IP地址:** 108.59.11.62 **国家:** 美国 **地区:** 哥伦比亚特区 **城市:** 华盛顿 **纬度:** 38.895390 **经度:** -77.039474 **查看:** Google 地图
vid.applovin.com	安全	否	**IP地址:** 34.160.64.118 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
www.appsgeyser.com	安全	否	**IP地址:** 172.67.168.94 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
sdkm.w.inmobi.com	安全	否	**IP地址:** 35.212.101.248 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
schemas.applovin.com	安全	否	No Geolocation information available.

www.inmobi.com	安全	否	**IP地址:** 20.81.69.107 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
google.com	安全	否	**IP地址:** 172.217.14.78 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
i.w.inmobi.com	安全	否	**IP地址:** 13.212.2.100 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
ads.appsgeyser.com	安全	否	**IP地址:** 199.115.116.164 **国家:** 美国 **地区:** 哥伦比亚特区 **城市:** 华盛顿 **纬度:** 38.895390 **经度:** -77.039474 **查看:** Google 地图
rt.applovin.com	安全	否	**IP地址:** 34.117.147.68 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
push.appsgeyser.com	安全	否	**IP地址:** 107.20.182.195 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
dock.inmobi.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://www.startappexchange.com/tracking/adclick • http://ltf.startappexchange.com/1.4/ • http://www.startappexchange.com/1.4/	com/startapp/android/publish/model/MetaData.java
• http://www.dummy.com	com/startapp/android/publish/nativead/NativeAdDetails.java

• http://www.inmobi.com/products/sdk/#downloads	com/inmobi/commons/a/b.java
• https://sdkm.w.inmobi.com/user/e.asm • http://dock.inmobi.com/carb/v1/i • http://dock.inmobi.com/carb/v1/o	com/inmobi/signals/q.java
• file:///android_res/	com/chartboost/sdk/impl/at.java
• http://www.appsgeyser.com? • http://www.appsgeyser.com	com/wsollys/ui/views/AboutDialog.java
• http://twitter.com/home?status= • https://m.google.com/app/plus/x/?v=compose&content= • https://www.facebook.com/dialog/feed?app_id=181821551957328&link=	com/inmobi/rendering/mraid/n.java
• http://tm.inmobi.com/telemetry-collector/v1/collect	com/inmobi/commons/core/c/c.java
• https://androidads23.adcolony.com/configure	com/jirbo/adcolony/c.java
• http://schemas.applovin.com/android/1.0	com/applovin/adview/AppLovinAdView.java
• https://play.google.com • http://play.google.com	com/startapp/android/publish/c/c.java
• http://www.startappexchange.com/tracking/infoevent	com/startapp/android/publish/d/a.java
• http://d1byvlfiet2h9q.cloudfront.net/inapp/resources/adinformationdialog3.html	com/startapp/android/publish/adinformation/AdInformationConfig.java
• http://www.startappexchange.com/tracking/adimpression	com/startapp/android/publish/d.java
• http://google.com/complete/search?output=toolbar&q=	com/wsollys/suggestions/SuggestionsClient.java
• javascript:chartboost.eventhandler.handlenativeevent(	com/chartboost/sdk/impl/bu.java
• https://inmobisdk-a.akamaihd.net/sdk/500/android/mraid.js • http://i.w.inmobi.com/showad.asm	com/inmobi/ads/b.java
• http://config.inmobi.com/config-server/v1/config/secure.cfg	com/inmobi/commons/core/configs/e.java
• 2.0.68.4	com/immersion/hapticmediasdk/HapticMediaSDKVersion.java
• http://market.android.com/	com/chartboost/sdk/impl/bb.java
• http://silvermob.com/marketplace/api/sdk/track/timeout/ • http://silvermob.com/marketplace/api/sdk/track/view/ • http://silvermob.com/marketplace/api/sdk/track/request?pid= • http://silvermob.com/marketplace/api/sdk/track/served/	com/silvermob/sdk/AdManager.java
• https://play.google.com • http://www.startappexchange.com • http://play.google.com	com/startapp/android/publish/h/v.java
• http://silvermob.com/marketplace/api/sdk/checkin?pn=	com/silvermob/sdk/MediationRulesManager.java

• http://rt.applovin.com/pix • http://a.applovin.com/ • https://vid.applovin.com/,https://pdn.applovin.com/,https://img.applovin.com/,https://d.applovin.com/,https://assets.applovin.com/,https://cdnjs.cloudflare.com/,http://vid.applovin.com/,http://pdn.applovin.com/,http://img.applovin.com/,http://d.applovin.com/,http://assets.applovin.com/,http://cdnjs.cloudflare.com/ • http://d.applovin.com/	com/applovin/impl/sdk/bx.java
• https://live.chartboost.com	com/chartboost/sdk/impl/ba.java
• http://www.appsgeyser.com/ads/landing.php • http://iccto.net/ • http://app2ad.com/?q= • http://stat.appsgeyser.com/ • http://www.appsgeyser.com/ • http://ads.appsgeyser.com/ • http://push.appsgeyser.com/ • http://iccto.com/ • http://www.appsgeyser.com/report/?app=app_id • http://ads.appsgeyser.com/checkstatus.php • http://splash.appsgeyser.com/ • http://updapp.com/ • http://www.appsgeyser.com/paused/	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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所关联的文件。

邮箱地址敏感信息提取

EMAIL	源码文件
softomate@softomate.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
AdColony	Advertisement	https://reports.exodus-privacy.eu.org/trackers/90
AppLovin (MAX and SparkLabs)	Advertisement, Identification, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/72
ChartBoost		https://reports.exodus-privacy.eu.org/trackers/53
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Inmobi		https://reports.exodus-privacy.eu.org/trackers/106
Nexage		https://reports.exodus-privacy.eu.org/trackers/33
Startapp	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/195

敏感凭证泄露检测

可能的密钥
AppLovin广告SDK的=> "applovin.sdk.key" : "-ZSF2wakygzAiT2ruKb6qE7Of7o4QhWOGzeIuE0qv--bX0RQL2WAGdZxmL_A2VZISDaLRb9KZ8x69MWUO1effC"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Passwort"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"

"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"

本报告由南明离火移动安全分析平台生成

"username" : "Name"
"password" : "Password"
"username" : "Nombre"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
"username" : "Name"
"password" : "Password"
Rm3kPC7ii9O6xx5NzKs8XGrNOZfaxCw4zB70goJXehA4Gy3oxwq36x71Cn7KxcAFeIEfVhbOVk9S
Ok9yaWdpbmFsRG9jdW1lbnRJRD0ieG1wLmRpZDpGQkU5MjA4OTBDMjA2ODExODA4M0YyQ0E4QjA4
0Is1LgSOVaPgZ9OYMaTYPrQhhmcuBo04r+BG3QtfpgGUeBY66hhEUOw1dauHWGRdVjuWTdLxd+ltu
Pc4bLrEJuc5GWxxYp4bwoYxwqVgWfQEMC3a7WHL4xkkX2t8BT/523hMXiswDG0EHAxxpqwftjAAl
NTJCNjI0NTY5OCIgeG1wOkNyZWF0b3JUb29sPSJBZG9iZSBQaG90b3Nob3AgQ1M2IChNYWNpbnRv

Ok9yaWdpbmFsRG9jdW1lbnRJRD0ieG1wLmRpZDpGRUU5MjA4OTBDMjA2ODExODA4M0YyQ0E4QjA4
bUBWYjSWU2Y2m8Ank40jRSIc1uhqSV/E7E5zO5feXMTddbAIjbIQPSK5cRhtQBctQupB2hSoJkxH
Be7QrsqPmAw+/mGKt1rfE4xUyqIbwDhIMrm+gI9R36osBPfr7AZBjsXYdbRbryI6ifGz3sLxbs24
vaDO2J17VOrNdi+J04px1GM3Cu2ENj7I+3r1JrM9Vvhyq6GXYCVafJjEhfBBEzBLoVcZkyI0+zT7
Ok9yaWdpbmFsRG9jdW1lbnRJRD0ieG1wLmRpZDpGNEU5MjA4OTBDMjA2ODExODA4M0YyQ0E4QjA4
Ok9yaWdpbmFsRG9jdW1lbnRJRD0ieG1wLmRpZDpGOUU5MjA4OTBDMjA2ODExODA4M0YyQ0E4QjA4
BykSfu+BL2CRrGixnkcVkhmPJtfa/UQiPWfZZ52s6BYOEK4QY8UgMxaC34CVCv72s99vL2y4ScYq
X+wupr62RM8Hr5mUZwRZsKjwH3CSigItbN0suXoUkh07VFPwZafOPXbS4XujrMsBztP/fb6Ijp0w
M0I1MCIgeG1wTU06RG9jdW1lbnRJRD0ieG1wLmRpZDo2MzBFQTlFNjYxMjAxMUUzQjhCRkRDNTJC
N3hs1m5l8jHVRki0jIbXqcByVfEGuKx4xLMcZOMkeMQCTq86Kx4xit6vmXWzOFTdVBCi33nDFsIF
aADPWGT8Fd9c4vgpI44VhxD7jTPfF+hni9CHopDo/1X0TwEGAMn4kfWfS4oUAAAAAElFTkSuQmCC
PrAAfAOjoAd0kqG5Fl0DjoA6kEuRA2Ccv9P5fyDmfBu4CG6CabFqJdomW0Fb9E97Dc6CWrAYpMYd
URTHnU1NzI9Wi1y31jCiNfMjwhL6sqSHSOwhInoq+vA1qtdAeq8ee4p6KKynCvIhsEwLEgrKiFX3
bWFnZVJlYWR5ccllPAAAA2hpVFh0WE1MOmNvbS5hZG9iZS54bXAAAAAAADw/eHBhY2tldCBiZWdp
n8P5xAz+rr7J3ukeerw1CgW/BBfBcwNl0scpJCXaR+fsViBWzNdLoJHjykY5TbLHSJd3gKtZockV
87gToILv2ETXq/LvCnAItNAuDI4lKA1bQIpUT+XO1cAt12BEFmLQNcW41SuUqYh26mvAJXCZxfc5
eD0iYWRvYmU6bnM6bWV0YS8iIHg6eG1wdGs9IkFkb2JlIFhNUCBDb3JlIDUuMy1jMDExIDY2LjE0
ZIMNYAmIBZNgFHSCFtAMWsHMbIl2gW2gDGwHUfz/CBgE4yA8xIMkEMHr7eAmuAU+2BpZiLZBPmjS
NTY2MSwgMjAxMi8wMi8wNi0xNDo1NjoyNyAgICAgICAgIj4gPHJkZjpSREYgeG1sbnM6cmRmPSJo
b3VyY2VSZWYjIiB4bWxuczp4bXA9Imh0dHA6Ly9ucy5hZG9iZS5jb20veGFwLzEuMC8iIHhtcE1N
39GluvWwGycKpL6SS4VOhU6FttX+CjAAgpoINtDHo/4AAAAASUVORK5CYII=
63zvDVq4pJyL3wYrphfCLFwDn0NYNxFjsqK1q0y2SewOuAFqw9iuRDqfEdnp0Q98IEex2HHQAEo5
MC9tbS8iIHhtbG5zOnN0UmVmPSJodHRwOi8vbnMuYWRvYmUuY29tL3hhcC8xLjAvc1R5cGUvUmVz
OIJERj4gPC94OnhtcG1ldGE+IDw/eHBhY2tldCBlbmQ9InIiPz6uekVTAAADwElEQVR42uyZXUgV
bZFPoY2B4JM+ONOh32MEm3x6NDZhYWhp8TA6wiu9YJLdSjRytNp5I97BTh8ekaNasT+zGzqs1Xay
wHmQZFC0gyvufaOixdR4KJkkiGgtCjnfYwwIrwF9IE7ve71+OhVksHKoiEJwBzxlJygTbWzEsmVN
UL94q7CdKIraOn/A4RdFBajAYZRpJT6i2VlEQ2qW5ufGIvkpbuDJVDM4r+vTk60rjbG2WFPLDI3L
C10F7968CFE2C76AC6F0650C877806D4514DE58FC239592D2385BCE5609A84B2A0FBDAF29B05505EAD1FDFEF3D7209ACBF34B5D0A806DF18147EA 9C0337D6B5B
cQhUgxQTycdS4ANnjC7jqcDLHkRG9BjFCtt0FxRY6PJOcqxcM86lDvziBYQ7Lo9JRBtbbrEtFe1o
dGlvbiByZGY6YWJvdXQ9IiIgeG1sbnM6eG1wTU09Imh0dHA6Ly9ucy5hZG9iZS5jb20veGFwLzEu

M0I1MCIgeG1wTU06RG9jdW1lbnRJRD0ieG1wLmRpZDo2MzBFQTlFQTYxMjAxMUUzQjhCRkRDNTJC
c2gpIj4gPHhtcE1NOkRlcml2ZWRGcm9tIHN0UmVmOmluc3RhbmNlSUQ9InhtcC5paWQ6MDY4MDEx
MkiCvaSBIdAPkgMRnUvBj4Is2Esxx7ttV7QlW81gjI/PzE6ErF2SorLBRj82Nyg8147oAnY+bWET
NjI0NTY5OCIgeG1wTU06SW5zdGFuY2VJRD0ieG1wLmlpZDo2MzBFQTlFOTYxMjAxMUUzQjhCRkRD
aYwSyk8tkPPpfHAY7ODvftAE2sAA82FxJp0AUnngnk7bHnAF1IEvs/ElIJ3CxcH6WhBnYDMFekEj
c2gpIj4gPHhtcE1NOkRlcml2ZWRGcm9tIHN0UmVmOmluc3RhbmNlSUQ9InhtcC5paWQ6QTlBRDI1
bMFq5CETP9GHdrzGc/Q7PVnAwegxG8dwEhvwB53owSBGkY18lGIpwmhGA17aTm2EtqECHzGGuziA
EvgxxWS9Elw3uTYECkG3gr+v/Bvje8FMtMak3qUwiBvkmFxbCPYqpvreomJGtggQb20vNw+ZRyni
cJ/EmvYoLl8j7JMlu6avMeNKkHDuNonDwybCqyRFXwWTRkWGWYdyDpAnMcNGgt+CVeBUADP+CnQZ
OTIwODkwQzIwNjgxMTgwODNGMkNBOEIwODNCNTAiLz4gPC9yZGY6RGVzY3JpcHRpb24+IDwvcmRm
BqQgPWjjUHyWmhDr4m6riNeSC5gl0RoHQQ8Tt4JKJk8MMWfFlDrKWq6tmCcM+kbp6hFpY303nYiL
BXH2z0QJatAT+dduocjO+a3+Qw4addLbWGfjpFk4jq8YxEEvQ+fjDYZwyOYdijUP1/UBVHsReiG6
n3nMsiI6GneUNHXjheC5Rh8z+o8XbU5nrobDHE5rSKMPc4QnrYj+xAuLNRwuA2ngpUYf[illegible]xF9
URiG1dW1H0szrazwF9O0ItmEDBOW8qKopC66qKiIgiDKLkKCfgiJIArSLuyiQsoMI[illegible]ylE
CEWGLRSoWG5Cptt36Le0iO7OdQdhD3wY0XHmNztzzpzz30AkEkmbbi[illegible]U6Dgtw6XjrMdW
eXzsMn0Ee1sjiDTxnUObShXRJRJxM5ozayXcDT4aXG9jtDDzPYc3+[illegible]5N4ucyE1+o2DX1r
c2gpIj4gPHhtcE1NOkRlcml2ZWRGcm9tIHN0UmVmOmluc3RhbmNlSUQ9InhtcC5paWQ6[illegible]MDEx
OlJERj4gPC94OnhtcG1ldGE+IDw/eHBhY2tldCBlbmQ9InIiPz77LxwAAADm0lEQVR42uyZXUgU
TEKyEjRxrFsg3g7RTtDAJBck76wMxznmE5CgW[illegible]5lkdhgdoBx3nmnKtGnKrNDYI1kpjjugrR
NjI0NTY5OCIgeG1wTU06SW5zdGFuY[illegible]RDOieG1wLmlpZDo2MzBFQTlFMTYxMjAxMUUzQjhCRkRD
WWVmeoia2gmaJRLlBP7HM1Bm[illegible]Xejaagco6LXU8ROSdH+IOF+YpsVjkWXRJrboU68AjyStXOiaC0G
wHlwF3xU3LtvZid4E+REOCaLn5myopNEywp6bTAdD[illegible]AYtlBzb/31QmtZU2RFxwe5DrtCTMFq8BYU
NjI0NTY5OCIgeG1wTU06SW5zdGFuY2VJRD0ieG1wLmlpZDpDNDMxMTM3QTYxMjAxMUUzQjhCRkRD
MTgxMDIwNjgxMTgwODNGMkNBOEIwODNCNTAiLHN0UmVmOmRvY3VtZW50SUQ9InhtcC5kaWQ6RkVF
frUf4C7YA[illegible]SCCdmJSokEi2Ao8olP[illegible]NJtFcaX1VsDKjhoBPgDFiu6EPcRBF4QT+tIDNYouPB
MzMrWc20D63NaPvf+g8svyYz584cxV74McvOnHv+c++dueecMaLRaMq/1oyk6KRod0Xng7WgAqwB
Wi5OoDHecBsvtNF7r6PktytRm6Ft5sQyBWaZLA5Va9+rTipMl3WrGkyEfoeOmJEn2kbVPzrUV6Zq
dHRwOi8vd3d3Lnczi[illegible]9yZy8xOTk5LzAyLzIyLXJkZi1zeW50YXgtbnMjIj4gPHJkZjpEZXNjcmlw
c2gpIj4gPHhtcE1NOkRlcml2ZWRGcm9tIHN0UmVmOmluc3RhbmNlSUQ9InhtcC5paWQ6MDM4MDEx
RQdAL5gAOxwQG0uQS+Yr2OyUaC87fQ/KHBZssgg85qCUOSH6OpgGG1wSbFIABkAILNQRfZhr+KDL

E72409364B865B757E1D6B8DB73011BBB1D20C1A9F931ADD3C4C09E2794CE102F8AA7F2D50EB88F9880A576E6C7B0E95712CAE9416F7BACB798564627846E93B
M0I1MCIgeG1wTU06RG9jdW1lbnRJRD0ieG1wLmRpZDpDNDMxMTM3NzYxMjAxMUUzQjhCRkRDNTJC
s9UHUbW7XNtHhU5V/WNQY5T3gExwzW4J4Qz4zvzQboDUwIxbEnOojL8PtEviaRVaToIrs5S1xIel
q+A3VbxxEnifyhLGYnajI2Wx6OLzGwZwzkb4bXiki2/CIq9rebEr7EsIq0zWpOe9VOWuoPabiULs
NzQwNzIwNjgxMTgwODNBRjJCNzQzNDlDQ0IiIHN0UmVmOmRvY3VtZW50SUQ9InhtcC5kaWQ6RkJF
J+ABYuAFlBusBW6QD0ZAHajhUzAeQrRBtoOuwL94ANwgVuI8B9gA6nnud7DXRH5DosVTucyELaDY
HCsOpIMlIIH/84I+0A1+TxXR88EWsAuUgWTgnHCMHwyDVvAINIFBK0mjTVaPRHAMVIJF4At4AdrB
CAMtgpJAS/JvLY2ldpXtPfQOLTK7e2bmjCj4wcOiO3O+d2bOfud7z0QHAoGo6RYxUdMwZkRPVsQq
URzHcddVu4hIFwvTsKToZhZRPlVQgdFDQReyQui1XgLBSirwQXqLwvC1EKIgrMgKgkIfoqALimFa
bj0i77u/IiBpZD0iVzVNME1wQ2VoaUh6cmVTek5UY3prYzlkIj8+IDx4OnhtcG1ldGEgeG1sbnM6
gk2q6O+8VLSasjFwS1PEaps2pym8SiK6kcarhIJLaT8O8m3YZYM3oNmu6CwwApo0RtnPDaSV/dmx
M0I1MCIgeG1wTU06RG9jdW1lbnRJRD0ieG1wLmRpZDpDNDMxMTM3QjYxMjAxMUUzQjhCRkRDNTJC
Ew70EKy2+ZT04g+B75yAYqdFLwYvKfgEH3uYQ2SBbvoudUq0WBJP6fSAg2L1rADvwBTY7IToCxR8
yoegUsOhuuEpMKbRh0qQf4I+K6J/gEegmompVLSarWEN0bWgN+YtMqPoFGbKAY3RDlKwdHPKA9tA
OlJERj4gPC94OnhtcG1ldGE+IDw/eHBhY2tldCBlbmQ9InIiPz7tuMs8AAADCElEQVR42uzZW0gU
NzQwNzIwNjgxMTgwODNBRjJCNzQzNDlDQ0IiIHN0UmVmOmRvY3VtZW50SUQ9InhtcC5kaWQ6RjlF
rHNYsC+mRFbvdFksyCpThG8HwwHBO5nEqtLYLrcKkCqrvspRUQ+2C8WW82FTrYMz6VrV1GQ1M+0o
bEOJ1dCLFTrkU+hezQrTrYTOVuiwT6GNeXgOglZCj2sb9Cl0MN7wOFXoIY2vc30KPR8DWIiYDt2n
NjI0NTY5OCIgeG1wTU06SW5zdGFuY2VJRD0ieG1wLmlpZDpDNDMxMTM3NjYxMjAxMUUzQjhCRkRD
QRTHvX5lGZVCWkpUWlhU+HD9qAcRNlcyQaV6sYfoQYKw8qUgK4LnWmU9JhW0AfkQ4UFERFCL2Jh
NzQwNzIwNjgxMTgwODNBRjJCNzQzNDlDQ0IiIHN0UmVmOmRvY3VtZW50SUQ9InhtcC5kaWQ6RjRF

免责声明及风险提示: