



ANDROID 静态分析报告



◆ PANEL_FF • v1.0

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-26 18:25:40

i应用概览

文件名称:	p.apk
文件大小:	23.32MB
应用名称:	PANEL_FF
软件包名:	com.sisuryaofficial.april1
主活动:	com.kcstream.cingmoe.MainActivity
版本号:	1.0
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	65/100 (低风险)
杀软检测:	24 个杀毒软件报毒
MD5:	94b9f1707ee13671a57adcf4ddaa7ee7
SHA1:	03cc58f273a6a9d418bfde609d31e9bb57d0e8f
SHA256:	753d76bf419a35efadd2529665908c78b045f7b7e7e17da8111b0fa8e8e6358

分析结果严重性

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
0	7	2	2	0

四大组件信息

Activity组件: 3个, 其中export的有: 1个
Service组件: 2个, 其中export的有: 0个
Receiver组件: 1个, 其中export的有: 1个
Provider组件: 1个, 其中export的有: 0个

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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
 签名算法: rsassa_pkcs1v15
 有效期自: 2008-02-29 01:33:46+00:00
 有效期至: 2035-07-17 01:33:46+00:00
 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
 序列号: 0x936eacbe07f201df
 哈希算法: sha1
 证书MD5: e89b158e4bcf988ebd09eb83f5378e87
 证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
 证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
 证书SHA512:
 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

公钥算法: rsa
 密钥长度: 2048
 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
 找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.BIND_DEVICE_ADMIN	签名	绑定设备管理	允许持有对象将意向发送到设备管理器。普通的应用程序一律无需此权限。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意应用程序可以用它来确定您所在的位置。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。

android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
-----------------------------	----	------	---

🔒 网络通信安全

序号	范围	严重级别	描述
----	----	------	----

📄 证书安全分析

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	应用程序使用代码签名证书进行签名

🔍 MANIFEST分析

高危: 0 | 警告: 3 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP、FTP协议，DownloadManager和Media Player。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性、真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过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	Broadcast Receiver (com.kcstream.cingmoe.AlarmReceiver) 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。

🔍 安全漏洞检测

高危: 0 | 警告: 3 | 信息: 1 | 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
2	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

3	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: MST G-STORAGE-3	升级会员: 解锁高级权限
4	向Firebase上传文件	警告		升级会员: 解锁高级权限

行为分析

编号	行为	标签	文件
00192	获取短信收件箱中的消息	短信	升级会员: 解锁高级权限
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
00202	打电话	控制	升级会员: 解锁高级权限
00080	将录制的音频/视频保存到文件	录制音视频文件	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
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
00101	初始化录音机	录制音视频	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
00199	停止录音并释放录音资源	录制音视频	升级会员: 解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员: 解锁高级权限
00136	停止录音	录制音视频命令	升级会员: 解锁高级权限
00194	设置音源 (MIC) 和录制文件格式	录制音视频	升级会员: 解锁高级权限
00090	设置录制的音频/视频文件格式	录制音视频	升级会员: 解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	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
00006	安排录制任务	录制音视频	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
00138	设置音频源 (MIC)	录制音视频	升级会员: 解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频文件	升级会员: 解锁高级权限
00133	开始录音	录制音视频命令	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
00041	将录制的音频/视频保存到文件	录制音视频	升级会员: 解锁高级权限

00128	查询用户账户信息	信息收集 账号	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
00054	从文件安装其他APK	反射	升级会员: 解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	10/30	android.permission.CALL_PHONE android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.READ_SMS android.permission.READ_CONTACTS android.permission.READ_CALL_LOG android.permission.ACCESS_FINE_LOCATION android.permission.GET_ACCOUNTS android.permission.SET_WALLPAPER android.permission.SEND_SMS
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.BIND_DEVICE_ADMIN android.permission.FOREGROUND_SERVICE

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。

域名检测

域名	状态	中国境内	位置信息
api.db-ip.com	安全	否	IP地址: 104.26.4.15 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
apkfromhelltoyouforthisthisweb.app	安全	否	IP地址: 199.36.158.100 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

surxratprivate-default-rtdb.firebaseio.com	安全	否	IP地址: 34.120.206.254 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
--	----	---	---

URL链接分析

URL信息	源码文件
<ul style="list-style-type: none"> https://apkfromhelltoyouforthis.web.app/ 	com/kcstream/cingmo/UpdateActivity.java
<ul style="list-style-type: none"> https://drive.google.com/uc?id= https://api.db-ip.com/v2/free/self https://script.google.com/macros/s/akfycbxy5tcqw9zxmrxnsut8v2pmpgha7obl2hz7-cvx0jn1hjy3fz2znh0sddb-nkay0vni/exec https://script.google.com/macros/s/akfycbwwbg7nhisk1o9bs8w4xrhoa0wkivytpaq2nw5owux_njka1folhvnky6vimpiho80v1w/exec 	com/kcstream/cingmo/MainActivity.java
<ul style="list-style-type: none"> https://surxratprivate-default-rtdb.firebaseio.com 	自研引擎-S

FIREBASE数据库分析

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://surxratprivate-default-rtdb.firebaseio.com 的 Firebase 数据库进行通信
Firebase远程配置已禁用	安全	Firebase远程配置URL (https://firebase-remoteconfig.googleapis.com/v1/projects/517916684441/namespaces/firebase:fetch?key=AlzaSyDI_MzYS51JhFyeY7IT2oPt9D0z_3OILcc) 已禁用。响应内容如下所示 <pre>{ "state": "NO_TEMPLATE" }</pre>

第三方SDK

SDK名称	开发者	描述信息
Google Play Service	Google	借助 Google Play 服务, 您的应用可以利用由 Google 提供的最新功能, 例如地图, Google+ 等, 并通过 Google Play 商店以 APK 的形式分发自动平台更新。这样一来, 您的用户可以更快地接收更新, 并且可以更轻松地集成 Google 必须提供的最新信息。
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关联的文件。
Jetpack App Startup	Google	App Startup 库提供了一种直接, 高效的方法在应用程序启动时初始化组件。库开发人员 and 应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序, 而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。

<p>Firebase</p>	<p>Google</p>	<p>Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。</p>
-----------------	-------------------------------	---

✉ 邮箱

EMAIL	源码文件
tiktok@sisuryaofficial.mp	com/kcstream/cingmoe/MainActivity.java

🔑 密钥凭证

可能的密钥
"firebase_database_url" : "https://surxratprivate-default-rtdb.firebaseio.com"
"google_api_key" : "AlzaSyDI_MzYS51JhFyeY7IT2oPt9D0z_3OILcc"
"google_app_id" : "1:517916684441:android:6ebf1a61bc4ca8fe8e0808"
NJKAUFolhnVKy6VimpiHO80v1w/exec

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成