南明离火
移动应用检测平台

ANDROID 静态分析报告

□□□□□

分析日期: 2025-04-30 14:26:22

应用概览

文件名称:	□□□□□ v□□□.apk
文件大小:	20.73MB
应用名称:	□□□□□
软件包名:	mistr_ial.ponds.wools.road
主活动:	com.wish.defaultcallservice.activity.ValidActivitySKV
版本号:	
最小SDK:	21
目标SDK:	31
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	52/100 (中风险)
杀软检测:	23 个杀毒软件报毒
MD5:	7d47a1e10720f4487edd8c1e67799125
SHA1:	9618d688633780d4e289d2509466f473bc6855d9
SHA256:	c38338e86a2c075ad1e7386e1534fb162a1d8d743a4a44e31e840443a80e35d3

分析结果严重性

高危	中危	信息	安全	关注
2	15	2	2	0

四大组件信息

Activity组件：5个，其中export的有： 3个
Service组件：8个，其中export的有： 3个
Receiver组件：2个，其中export的有： 2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: False
v4 签名: False
主题: C=XjaC1Zs, ST=UMc9ZXHXkJ, L=GmCd9, O=mgEEcnNHV0, OU=3oBz7, CN=LFtGbGa
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-01 09:36:49+00:00
有效期至: 2025-06-30 09:36:49+00:00
发行人: C=XjaC1Zs, ST=UMc9ZXHXkJ, L=GmCd9, O=mgEEcnNHV0, OU=3oBz7, CN=LFtGbGa
序列号: 0x735822ab
哈希算法: sha256
证书MD5: ff03a1a414eca387f9c4f4fa656aad79
证书SHA1: a4489d533773b1e0befa8abd6b0b7b9274f9f4fc
证书SHA256: 1b3ed4d71ea4779172e70c3de5ddd5b63077974aa22c82e77542fcebac48d0ef
证书SHA512:
a449553b5e176537701ad3fcd779aa7e6534617614b1034c28170c414b69785ee6f2a5b338763e5e832c4aad2f8027ad2b2713c67a2a67548d7e015a36573ddd

公钥算法: rsa
密钥长度: 2048
指纹: 43291b6db2f02a7ec1a0bd01695d7bb0dd08bc6b7253d2bff3973f8bb3998d47
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.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.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。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android 8.0 以上系统允许安装未知来源应用程序权限。
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.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.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。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。

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: **9** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity (com.wish.defaultcallservice.activity.TestCallActivitySKV) 未被保护。 [android:exported=true]	警告	发现 Activity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。
2	Activity (com.wish.defaultcallservice.activity.GoogleActivitySJKV) 未被保护。 [android:exported=true]	警告	发现 Activity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。
3	Activity (com.wish.defaultcallservice.activity.ConfirmationIntentWrapperActivitySJKV) 未被保护。 [android:exported=true]	警告	发现 Activity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。
4	Service (com.wish.defaultcallservice.service.AutoServiceSJKV) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	发现一个 Service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	Service (com.wish.defaultcallservice.service.ShellService) 未被保护。 [android:exported=true]	警告	发现 Service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。
6	Broadcast Receiver (com.wish.defaultcallservice.hellodaemon.WakeUpReceiverSKV) 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.wish.defaultcallservice.hellodaemon.WakeUpReceiverSKV$WakeUpAutoStartReceiver) 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。
8	Service (com.wish.defaultcallservice.hellodaemon.JobSchedulerServiceV) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service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。
9	高优先级的Intent （1000） - 这个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

安全漏洞检测

高危: **2** | 警告: **5** | 信息: **2** | 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	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	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
4	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
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	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
7	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
8	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
9	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

10	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	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-2	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
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
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
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
00035	查询已安装的包列表	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
00125	检查给定的文件路径是否存在	文件	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
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
00167	使用辅助功能服务执行在活动窗口中获取 root 的操作	无障碍服务	升级会员：解锁高级权限
00160	使用辅助服务执行通过视图 ID 获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 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
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
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

00191	获取短信收件箱中的消息	短信	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	2/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	4/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE 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
ysee5i35id.com	安全	否	No Geolocation information available.

URL链接分析

URL信息	源码文件
• https://drive.google.com/file/d/1iz7b_8xcawz4jhuujyxz2fbvgmcfryod/view?usp=share_link • http://ysee5i35id.com	com/wish/defaultcallservice/activity/GoogleActivitySJKV.java
• https://drive.google.com/file/d/1iz7b_8xcawz4jhuujyxz2fbvgmcfryod/view?usp=share_link	com/wish/defaultcallservice/activity/MainActivitySJKV.java
• https://drive.google.com/file/d/13sgolx8s3q9dio-	com/wish/defaultcallservice/BuildConfig.java
• https://drive.google.com/file/d/1e8k4fcjqvip_w5eoujm441vommjczzoo/view?usp=sharing • https://drive.google.com/file/d/1nx63g5z3snx-j2jcgkwmxvvim_ihli/view?usp=sharing • https://drive.google.com/file/d/1hzg40qw7dqgl2hf6tugkklkf5a0dnabt/view?usp=share_link	自研引擎-S

第三方SDK

SDK名称	开发者	描述信息
百度应用加固	Baidu	百度应用加固能够为 Android、Linux 等智能终端平台上的应用程序提供代码加密、完整性校验、反注入、反调试、运行时数据加密等各种安全能力，可以有效帮助智能终端上的应用程序抵御各种安全威胁。
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。

密钥凭证

可能的密钥
"str_key_agreement_submit_style" : "AGREEMENT_SUBMIT_STYLE"
MIGeE1ujgHRhlBUVGgLh9oOR7QC0aGxT
8xcAwZ4jhUUjyXz2fBvgmCfRYOd/view
ivB3TZ7pTnxffXWyDruV6nd4LBJWYiw3

免责声明及风险提示: