南明离火
移动应用检测平台

ANDROID 静态分析报告

Smile • v1.0.0

分析日期: 2025-04-30 16:30:08

应用概览

文件名称:	Smile v1.0.0.apk
文件大小:	2.55MB
应用名称:	Smile
软件包名:	com.weixin.smile
主活动:	activity.SplashActivity
版本号:	1.0.0
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:	43/100 (中风险)
杀软检测:	21 个杀毒软件报毒
MD5:	51dae4a168d05832415c54f60e608eb3
SHA1:	3d99f3f8350bb8bb786411aff6f20e547720f20d
SHA256:	07b826b26a86e97f49e1b17f59fd0c2c4bf354c78168389d18aad65cf45a3819

分析结果严重性

高危	中危	信息	安全	关注
5	11	1	2	0

四大组件信息

Activity组件：4个，其中export的有： 2个
Service组件：5个，其中export的有： 1个
Receiver组件：4个，其中export的有： 4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: False
v2 签名: True

v3 签名: False
v4 签名: None
主题: CN=Smile, OU=BJC, O=BJC, L=wuhan, ST=hubei, C=421123
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-21 17:02:55+00:00
有效期至: 2050-02-15 17:02:55+00:00
发行人: CN=Smile, OU=BJC, O=BJC, L=wuhan, ST=hubei, C=421123
序列号: 0x1
哈希算法: sha256
证书MD5: fabacc2065772206cc6a5c3a865f0697
证书SHA1: ab0b45e355d57531683751caf128ebcc01300626
证书SHA256: 609751a5cfe0b4a24b8b73a490831fd09c6d396c0b421922b08314c8ceefd5e3
证书SHA512:
a1b958500f231aa44b21a362ce124042aa86578775dbc02b89e6c6b01b8bd705c620acb40a7839a8afaade3f6ec5b93b4dab9328c0df5a42140a009d9b696ac2

公钥算法: rsa
密钥长度: 2048
指纹: 9d364695361de9966dc9a63357436e5a66fde7900321f2944cb65dcafc72f969
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.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.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.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
android.permission.USE_EXACT_ALARM	普通	允许在未经用户许可的情况下使用精确的警报	允许应用使用精确的警报。
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.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_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.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。
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
android.permission.READ_CONTACTS	危险	读取联系人信息	允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_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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可
android.permission.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
com.weixin.smile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览的Activity组件

ACTIVITY	INTENT
activity.ComposeSmsActivity	Schemes: sms://, smsto://, mms://, mmsto://,

网络通信安全

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

证书安全分析

高危: **0** | 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

MANIFEST分析

高危: **4** | 警告: **9** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
2	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。

3	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。
4	应用程序处于测试模式 [android:testOnly=true]	高危	它可能会暴露自身之外的功能或数据，这会造成一个安全漏洞。
5	Activity (activity.SplashActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而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"并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (23) 更新到 29 或更高版本以在平台级别修复此问题。
6	Activity (activity.alias) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而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"并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (23) 更新到 29 或更高版本以在平台级别修复此问题。
7	Activity-Alias (activity.alias) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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	Broadcast Receiver (receiver.BootReceiver) 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。
9	Broadcast Receiver (receiver.AlarmReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.android.alarm.permission.SET_ALARM [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。
10	Broadcast Receiver (receiver.SmsReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_SMS [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。
11	Broadcast Receiver (receiver.MmsReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_WAP_PUSH [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。
12	Activity (activity.ComposeSmsActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity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Activity是显式导出的。
13	Service (service.HeadlessSmsSendService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [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。

14	高优先级的Intent （2147483647） - {2} 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: **0** | 警告: **1** | 信息: **1** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
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: MSTG-STORAGE-3	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00049	查询短信发送者的电话号码	短信 信息收集	升级会员：解锁高级权限
00050	查询短信服务中心时间戳	短信 信息收集	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
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
00192	获取短信收件箱中的消息	短信	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
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	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
00033	查询IMEI号	信息收集	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
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
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
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	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
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00040	发送短信	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
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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.READ_SMS android.permission.SEND_SMS android.permission.RECEIVE_SMS android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE
其它常用权限	7/46	android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_NOTIFICATION_POLICY

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
snowy-shape-feab.lkcasy88888890.workers.dev	安全	否	**IP地址:** 172.67.197.182 **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
www.naver.com	安全	否	**IP地址:** 23.222.204.254 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 埃尔塞贡多 **纬度:** 33.919201 **经度:** -118.416580 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• 61.218.17.222	mqtt/MqttConfig.java
• https://snowy-shape-feab.lkcasy88888890.workers.dev/sub	service/RunningService.java
• https://www.naver.com/	activity/MainActivity.java

第三方SDK

SDK名称	开发者	描述信息
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高稳定性强。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

密钥凭证

可能的密钥
1569b25bb8b179d5ea5ab[illegible]331608dd1
9ccd73a516869a[illegible]6d53d895bdefd1

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。本平台对使用本产品及其内容所引发的任何直接或间接损