南明离火

——移动应用检测平台——

ANDROID 静态分析报告

赏帮赚 V5.2.7

分析日期: 2025-04-30 23:30:22

应用概览

文件名称:	赏帮赚 v5.2.7.apk
文件大小:	6.88MB
应用名称:	赏帮赚
软件包名:	com.sbzapp.sbz
主活动:	com.lt.app.MainActivity
版本号:	5.2.7
最小SDK:	19
目标SDK:	30
加固信息:	360加固
开发框架:	Java/Kotlin
应用程序安全分数:	44/100 (中风险)
杀软检测:	2个杀毒软件报毒
MD5:	e35d2a0fa4c825173d13ed0be08b87ee
SHA1:	77a4b71bd39e72c3eb981d686a06819b550bcb23
SHA256:	6f232ba569aad9c8a1bd589a4b7c95e97981807b6f90a69e3c6541870425b7fd

分析结果严重性

高危	中危	信息	安全	关注
2	2	0	1	0

四大组件信息

Activity组件：5个，其中export的有： 1个
Service组件：0个，其中export的有： 0个
Receiver组件：1个，其中export的有： 1个
Provider组件：2个，其中export的有： 0个

证书信息

没有签名，缺少证书
v1 签名: False
v2 签名: False
v3 签名: False
v4 签名: False

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.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.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。
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。
com.sbzapp.sbz.permission.YM_APP	未知	未知权限	来自 android 引用的未知权限。
com.sbzapp.sbz.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
com.lt.app.JumpActivity	Schemes: lapp288446://,

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: 1 | 警告: 0 | 信息: 0

标题	严重程度	描述信息
缺少代码签名证书	高危	未找到代码签名证书

MANIFEST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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/nsc]	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	Activity (com.lt.app.JumpActivity) 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	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。

安全漏洞检测

序号	问题	等级	参考标准	文件位置

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
00012	读取数据并放入缓冲流	文件	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	3/30	android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE

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。

第三方SDK

SDK名称	开发者	描述信息

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。

密钥凭证

可能的密钥
"http_auth_p" : "Password"

免责声明及风险提示: