南明离火
移动应用检测平台

ANDROID 静态分析报告

格式工厂 • v3.35

分析日期: 2024-05-26 12:18:16

应用概览

文件名称:	格式工厂.apk
文件大小:	83.86MB
应用名称:	格式工厂
软件包名:	com.geshi.formatfactory
主活动:	com.geshi.formatfactory.activity.SplashActivity
版本号:	3.3.5
最小SDK:	23
目标SDK:	27
加固信息:	360加固 加固
应用程序安全分数:	29/100 (重大风险)
跟踪器检测:	5/432
杀软检测:	4 个杀毒软件报毒
MD5:	99c04294e79f02572eb78b52434f745c
SHA1:	709636c51d391ee752deb74d[illegible]ed7ba07566
SHA256:	8bb523c4cb00b3315aaa[illegible]9200c7f9d5cbd144395[illegible]5bff4269d3a4f1479b59

分析结果严重性分布

高危	中危	信息	安全	关注
21	21	1	2	12

四大组件导出状态统计

Activity组件：70个，其中export的有： 3个
Service组件：13个，其中export的有： 3个
Receiver组件：1个，其中export的有： 0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: True
v3 签名: False
v4 签名: False
主题: C=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2021-06-15 10:06:29+00:00
有效期至: 2046-06-09 10:06:29+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1
序列号: 0x25b2f2cc
哈希算法: sha256
证书MD5: 83f9f8f6bb45fed6e236ebf2e87cc749
证书SHA1: 1b91c9196dda58ff751c0b3feb5e6c3d189819c0
证书SHA256: 6997471e06bc9d451948953e7ec5ade0ba1c6811f1d446360885e1fcde37a9f3
证书SHA512:
4eba247a2a1421e53121ebecfff39add5ddba42575cf657c9d5f80a07354ef3099a7d7863a41f44224bea1fd453c599d75e18c5b247c...23662968b15252df2b0

公钥算法: rsa
密钥长度: 2048
指纹: 1079520ce93adcc083c64b359824287962ad5c8a074fbcf251b26fc4c70eff6f
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
com.geshi.formatfactory.openadsdk.permission.TT_PANGOLIN	未知	未知权限	来自 android 引用的未知权限。
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.MANAGE_DOCUMENTS	签名	允许管理文档访问，通常在选择器中	允许应用程序管理对文档的访问，通常作为文档选取器的一部分。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.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。
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.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。
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.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。

com.google.android.apps.photos.permission.GOOGLE_PHOTOS	未知	未知权限	来自 android 引用的未知权限。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。

网络通信安全风险分析

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。

证书安全合规分析

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	应用程序已使用代码签名证书进行签名

Manifest 配置安全分析

高危: **16** | 警告: **12** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 6.0-6.0.1, [minSdk=23]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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MediaPlayer。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。
3	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。
4	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。
5	Activity （com.geshi.formatfactory.activity.MainActivity ） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。

6	Activity (com.geshi.formatfactory.activity.MainActivity) 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。
7	Activity （com.geshi.formatfactory.activity.OldMainActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
8	Activity （com.geshi.formatfactory.activity.MyWorkActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
9	Activity设置了TaskAffinity属性 (com.geshi.formatfactory.wxapi.WXPayEntryActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
10	Activity （com.geshi.formatfactory.wxapi.WXPayEntryActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
11	Activity (com.geshi.formatfactory.wxapi.WXPayEntryActivity) is vulnerable to StrandHogg 2.0	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 (27) 更新到 29 或更高版本以在平台级别修复此问题。
12	Activity (com.geshi.formatfactory.wxapi.WXPayEntryActivity) 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。
13	Activity设置了TaskAffinity属性 (com.geshi.formatfactory.wxapi.WXEntryActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
14	Activity （com.geshi.formatfactory.wxapi.WXEntryActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
15	Activity (com.geshi.formatfactory.wxapi.WXEntryActivity) is vulnerable to StrandHogg 2.0	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 (27) 更新到 29 或更高版本以在平台级别修复此问题。
16	Activity (com.geshi.formatfactory.wxapi.WXEntryActivity 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。

17	Service (com.geshi.formatfactory.service.FileFormatService) 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。
18	Service (com.geshi.formatfactory.service.NewFileFormatService) 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。
19	Service (com.geshi.formatfactory.service.RoomDataService) 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。
20	Activity (com.alipay.sdk.app.PayResultActivity) 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。
21	Activity （com.alipay.sdk.app.AlipayResultActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
22	Activity (com.alipay.sdk.app.AlipayResultActivity) is vulnerable to StrandHogg 2.0	高危	已发现启动存在 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”或设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 29 或更高版本以在平台级别修复此问题。
23	Activity (com.alipay.sdk.app.AlipayResultActivity) 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。
24	Activity （com.sobot.chat.conversation.SobotChatActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
25	Activity （com.bytedance.sdk.openadsdk.stub.activity.Stub_SingleTask_Activity_T） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
26	Activity （com.bytedance.sdk.openadsdk.stub.activity.Stub_SingleTask_Activity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
27	Activity （com.ss.android.downloadlib.activity.TTDelegateActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。

28	Activity （com.ss.android.downloadlib.activity.JumpKllkActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
29	Activity （com.ss.android.socialbase.appdownloader.view.DownloadTaskDeleteActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。
30	Activity （com.ss.android.socialbase.appdownloader.view.JumpUnknownSourceActivity） 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 (27) 更新到 28 或更高版本以在平台级别修复此问题。

代码安全漏洞检测

高危: **3** | 警告: **8** | 信息: **1** | 安全: **2** | 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
3	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
4	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
5	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

6	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
7	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
8	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	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
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	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
12	该文件是World Writable。任何应用程序都可以写入文件	高危	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
13	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	升级会员：解锁高级权限
14	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	arm64-v8a/libavutil.so	True info 二进制文件设置了NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

2	arm64-v8a/libnative-lib.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__memmove_chk', '__vsnprintf_chk', '__strlen_chk']	False warning 符号可用
3	arm64-v8a/libpangleflipped.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

4	arm64-v8a/libsobot.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.RECORD_AUDIO android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS
其它常用权限	5/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
apps.oceanengine.com	安全	是	**IP地址:** 222.186.18.193 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图

beta-app-api.pcgeshi.com	安全	是	**IP地址:** 112.74.75.195 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
h5.m.taobao.com	安全	是	**IP地址:** 222.186.18.193 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图
app-api.pcgeshi.com	安全	是	**IP地址:** 112.74.75.195 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
image.cnamedomain.com	安全	否	No Geolocation information available.
www.toutiaopage.com	安全	是	**IP地址:** 222.186.18.193 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
m.pcgeshi.com	安全	是	**IP地址:** 180.97.251.209 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
i.snssdk.com	安全	是	**IP地址:** 222.186.18.193 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
www.soboten.com	安全	是	**IP地址:** 222.186.18.193 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图

s.anjixg.com	安全	是	**IP地址:** 222.186.18.193 **国家:** 中国 **地区:** 上海 **城市:** 埃塞俄比亚 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
www.samsungapps.com	安全	否	**IP地址:** 52.18.136.34 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
sf6-ttcdn-tos.pstatp.com	安全	是	**IP地址:** 222.186.18.193 **国家:** 中国 **地区:** 浙江 **城市:** 台州 **纬度:** 28.666668 **经度:** 121.349998 **查看:** 高德地图
mobilegw.alipaydev.com	安全	是	**IP地址:** 10.75.132.131 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
www.chengzijianzhan.com	安全	是	**IP地址:** 222.186.18.193 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://image.[redacted]domain.com'! • http://oss-cn-[redacted]aliyuncs.com',or	e/a/c/a/a/d.java
• http://oss-cn-hangzhou.aliyuncs.com	e/a/c/a/a/f/b.java
• https://github.com/kongzue/dialogx/wiki	com/kongzue/dialogx/DialogX.java
• https://github.com/kongzue/dialogx	com/kongzue/dialogx/interfaces/BaseDialog.java
• https://github.com/kongzue/dialogx	com/kongzue/dialogx/impl/ActivityLifecycleImpl.java
• 203.107.1.1	e/a/c/a/a/f/h/f.java

• https://mobilegw.alipaydev.com/mgw.htm • https://loggw-exsdk.alipay.com/loggw/logupload.do • https://wappaygw.alipay.com/home/exterfaceassign.htm? • https://mcgw.alipay.com/sdklog.do • https://mclient.alipay.com/home/exterfaceassign.htm? • https://mobilegw.alipay.com/mgw.htm	e/b/b/c/j/a.java
• https://h5.m.taobao.com/mlapp/olist.html	e/b/b/c/k/a.java
• https://s.anjixg.com/sa.gif?project=gsgcan&remark=	e/l/b/q/e0.java
• https://wj.qq.com/s2/10358636/03b7 • https://wj.qq.com/s2/9759060/59af	e/l/b/q/m.java
• https://m.pcgeshi.com/useragreement • https://m.pcgeshi.com/privacypolicy	com/geshi/formatfactory/activity/AboutActivity.java
• https://app-api.pcgeshi.com/html/vip_service.html	com/geshi/formatfactory/activity/MemberCenterActivity.java
• https://wj.qq.com/s2/10549595/f35b/openid= • https://app-api.pcgeshi.com/html/vip_service.html	com/geshi/formatfactory/activity/NewMemberActivity.java
• https://www.samsungapps.com/appquery/appdetail.as?appid=	com/ss/android/downloadlib/g/h.java
• https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java
• https://work.weixin.qq.com/kfid/kfc917df190f4292c0f	e/l/b/q/v.java
• https://www.soboten.com	com/geshi/formatfactory/App.java
• https://m.pcgeshi.com/privacypolicy • https://m.pcgeshi.com/useragreement	e/i/a/k/n0.java
• https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
• https://work.weixin.qq.com/kfid/kfc9[illegible]f190f4292c0f	e/i/a/k/l0.java
• www.toutiaopage.com/tetris/page • https://apps.oceanengine.com/customer/api/app/pkg_info/ • www.chengzijianzhan.com	com/ss/android/downloadlib/addownload/compliance/b.java
• https://wj.qq.com/s2/9755451/c895	com/geshi/formatfactory/activity/OldMainActivity.java
• https://app-api.pcgeshi.com/ • https://beta-app-api.pcgeshi.com/	e/l/b/o/c.java
• http://image.cnamedomain.com'! • http://127.0.0.1 • http://oss.aliyuncs.com • http://oss-cn-***.aliyuncs.com',or	e/a/c/a/a/g/f.java
• https://m.pcgeshi.com/useragreement • https://m.pcgeshi.com/privacypolicy	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
FFmpeg	FFmpeg	FFmpeg 是领先的多媒体框架，能够解码，编码，转码，MUX，DEMUX，流式，过滤和播放人类和机器创建的几乎所有内容。
Pangle SDK	ByteDance	穿山甲是巨量引擎旗下全球应用变现与增长平台，合作优质媒体超 30,000 家，日请求突破 607 亿，日均展示达 100 亿，覆盖 7 亿日活用户，为全球应用和广告主提供高效的用户增长和变现解决方案。
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
C++ 共享库	Android	在 Android 应用中运行原生代码。
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
FFmpegKit	arthenica	FFmpegKit is a collection of tools to use FFmpeg in Android, iOS, Linux, macOS, tvOS, Flutter and React Native applications.
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 高效绘制、简单易用等优势。
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。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
智齿客服 SDK	智齿科技	智齿客服 SDK 是客服系统的客端的解决方案，既包含了客服聊天逻辑管理，也提供了聊天界面，开发者可方便的将客服功能集成到自己的 App 中。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
libYUV	Google	libYUV 是 Google 开源的 yuv 图像处理库，实现对各种 yuv 数据之间的转换，包括数据转换，裁剪，缩放，旋转。
支付宝 SDK	Alipay	支付宝开放平台通过支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
神策分析 SDK	神策	神策分析，是针对企业级客户推出的深度用户行为分析产品，支持私有化部署，客户端、服务器、业务数据、第三方数据的全端采集和建模，驱动营销渠道效果评估、用户精细化运营改进、产品功能及用户体验优化、老板看板辅助管理决策、产品个性化推荐改造、用户标签体系构建等应用场景。作为 PaaS 平台支持二次开发，可通过 BI、大数据平台、CRM、ERP 等内部 IT 系统，构建用户数据体系，让用户行为数据发挥深远的价值。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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。

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_CHANNEL" : "HuaWei"
"sobot_ding_cai_sessionoff" : "Fine della conversazione, nessun feedback"
"sobot_ding_cai_sessionoff" : "Conversation ended, you can't send feedback"
"sobot_ding_cai_sessionoff" : "Percakapan berakhir, tidak ada umpan balik"
"sobot_ding_cai_sessionoff" : "Perbincangan tamat, tidak dapat maklumbalas"
197e6e0f6b1617561be4022415969713
b3f27faa8282c119959b97b34cdddc24
af34ba0045955af340036a1b29d700b2
6d2951692b739d6beeb59de330b1ab19
b6cbad6cbd5ed0d209afc69ad3b7a617efaa9[illegible]3c[illegible]7eabe0be42d924936[illegible]78[illegible]801b1fd74b079e5ff9690061dacfa4768e981a526b9ca77156ca36251cf2f906d105481374998a7e6e6e18f75ca98b8[illegible]d2e[illegible]f86ff402c874cca0a2630[illegible]2[illegible]237858206867d210020daa38c48b20cc9dfd82b44a51aeb5db459b22794e2d649
MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgFOl7gCz[illegible]6q[illegible]2uBFFwHwVQbsUxDOobzclGPlOQcn+FfPXGTGJ06l1K2SA92m1pbt7eNljoa9yAwomSzaM+NXgiC4JEheZSdbSSIox7fvlP[illegible]B7[illegible]aVZkdvYhofEziTuvj[illegible]hz[illegible]sQ73V3/48sMZhmk0BzkTLkdVBQY0rA3PA8pRKJAgMBAAE=
uDarS1ccwTSWf7lT4V[illegible]vhGyn[illegible]ElitRdv
e6b1bdcb8905[illegible]2[illegible]19fe06d0fdf7628ad[illegible]83[illegible]52[illegible]a1ecfe991164711bbf9297e75353de96f1740695d07610567b1240549af9cbd87d06919ac31c859ad37ab6907c311[illegible]759e1e208775989a4[illegible]691[illegible]f4bbbc58174d2a96b1d0d970a05114d7ee57dfc33b1bafaf6e0d820e838427018b6435f903df04ba7fd34d73f843d[illegible]434b164e0220baabb10c8[illegible]3[illegible]4c6b7da79d8220a968356d15090dea07df9606f665cbec14d218dd3d691cce2866a58840971b6a57b76af88b1a65[illegible]080281a6ab20be5879[illegible]eb7ff70871ce684e7174ada5dc3159c461375a0796b17ce7beca83cf34f65976d237aee993db48d34a4e344f4d8b7e991[illegible]9168bdd7
6Z2e5bi45oqx5q2J77y[illegible]35YWz6Zet5omL5py65byA5Y+R6ICF5qih5byP77yMQXBw5Y2z5bCG5YWz6Zet
60d530b226a57[illegible]38922c
bec809930[illegible]d74e4[illegible]95c7424b4c565f6d
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC039jg7sotX4xr+LGdmTWs7TgRGTAiMAINpAX8B1r8qUbiyHpqp4ozlQhOI8ogMM+p1rcDWTvM+8Iwd9laClFUeVYaun+h4XUgIM5nQ1qmTVN3uf1lYZxzf2a8B0pHWxPYDwIyeHj2UEb3Cx5i5NG5cZ24depXP6jPKwyzTTJtEwIDAQAB
tStEWiXFQdOqDLbSqw9VhC5AgvTAI5tGZfZ5T

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

免责声明及风险提示: