南明离火
移动应用检测平台

ANDROID 静态分析报告

杏吧 • v1.35

分析日期: 2024-05-02 20:09:29

概述

文件名称:	tqrgxofm.apk
文件大小:	7.34MB
应用名称:	杏吧
软件包名:	com.google.ferrrr
主活动:	com.google.ferrrr.activity.inception.InceptionActivity
版本号:	1.35
最小SDK:	21
目标SDK:	30
加固信息:	360加固 加固
MD5:	2cb0ec521ea92fc4479976d370995d6f
SHA1:	5a3904c20522ce2f232eac7538627c9210dffb38
SHA256:	20e837cf6c4a6d8d89c0751890b973f076a42fe1a90b08e6c59821169e023dcd
应用程序安全分数:	49/100 (中风险)
杀软检测:	AI评估：安全

分析结果严重性

高危	中危	信息	安全	关注
3	11	1	2	0

四大组件信息

Activity组件：17个，其中export的有： 1个
Service组件：0个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0个
Provider组件：2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=kkk, ST=rt, L=tr, O=gfde, OU=htrre, CN=ltrt
签名算法: rsassa_pkcs1v15
有效期自: 2024-02-23 07:19:54+00:00
有效期至: 2051-07-11 07:19:54+00:00
发行人: C=kkk, ST=rt, L=tr, O=gfde, OU=htrre, CN=ltrt
序列号: 0x5251d39c
哈希算法: sha256
证书MD5: 7734e7219e3b52254302243c1c36bb55
证书SHA1: ff39f1819bdd46d1b2ccf143de29235d54271fea
证书SHA256: 6995be29bbf0bcf1f1d70dcf8a3f72c36f7b73c91248b7b096877a3dc9fdee73
证书SHA512:
21d6726c42a233e23a02e6b11606f7e57311d0dd339e2d485caf095d0636760bbba807c0ce72c847d51096bb89fec837e19f0db62e50f9689c982997a8dc56b0

公钥算法: rsa
密钥长度: 2048
指纹: 1ecbcf7640e8dd5372c0fc5a70f15952ef4bf663172a95d84c507743f7713a30
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.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.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.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_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.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。

网络安全配置

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分析

高危: **0** | 警告: **4** | 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 5.0-5.0.2, [minSdk=21]	警告	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.google.ferrrr.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，因此使其对设备上的任何其他应用程序都可访问。

</> 源代码分析

高危: **2** | 警告: **6** | 信息: **1** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
				a/a.java a0/a.java a0/d.java a0/j.java a0/o.java a1/a.java b1/i.java b1/k.java b1/n.java com/danikula/videocache/d.java com/danikula/videocache/f.java d/h.java d0/a.java f1/a.java f1/d.java f1/j.java h1/d.java h1/n.java h1/o.java h1/r.java j/c.java k/d.java k/f.java k/g.java k/h.java k/i.java k/k.java k/l.java k/m.java k/o.java k/r.java k/s.java k1/f.java l0/l.java

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	l0/n.java l0/o.java l0/p.java l0/q.java l0/r.java l1/d.java l1/k.java me/jessyan/autosize/AutoSize.java me/jessyan/autosize/AutoSizeConfig.java me/jessyan/autosize/DefaultAutoAdaptStrategy.java me/jessyan/autosize/utils/AutoSizeLog.java o/a.java o/c.java org/xutils/common/util/LogUtil.java p1/a.java q/d.java q0/a.java q1/c.java q1/f.java r0/c.java r1/e.java s/d.java t/c.java t/d.java t/e.java t/f.java t/i.java t0/c.java t4/e.java u/a.java u/e.java v0/i.java v0/j.java w/a.java w0/e.java w0/j.java x0/a.java y0/c.java y0/d.java y0/f.java y0/s.java y0/t.java z/b.java
2	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	org/xutils/common/util/MD5.java r1/f.java
3	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	org/xutils/x.java

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	com/jg/ids/i/i.java
5	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	com/danikula/videocache/d.java y1/b.java
6	启用了调试配置。生产版本不能是可调试的	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	org/xutils/BuildConfig.java
7	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	org/xutils/db/DbManagerImpl.java t1/a.java
8	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	a4/a.java z3/a.java z3/b.java
9	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	org/xutils/common/util/FileUtil.java
10	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	com/danikula/videocache/f.java

动态库分析

序号	动态库	NX(堆栈禁止执行)	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/librtmp-jni.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
2	arm64-v8a/libX86Bridge.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

滥用权限

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	4/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE

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。

网址

网址信息	源码文件
• 127.0.0.1 • http://%s:%d/%s	com/danikula/videocache/d.java
• http://%s:%d/%s	com/danikula/videocache/g.java
• 127.0.0.1	y1/b.java

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。
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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

密钥凭证

可能的密钥
mEIkzk1Ez0ozCF82LXUJpqeHyEqTewnXQhUkUVB3LJdCPvgOZX1lxDV3BjReOUwOnV4GMySaELIhx6SB5KdRiTPExC4rCcj6cch6rMFJTBhmEfMlRlvEqvxlLP2QWYOZ
b61a35d908f8e0adcd3fe7bebddb41ff214b5ccb
097176da-72b2-4f8c-8806-49fc80d3f502
98daac24d8054bb4bd0117e35a6876f1
694F193340AEC90CFFFD7636079EFC20

3d76d893f141415ca9deedb77db70926
63db6d9de4b085594253d520
5eb9245b5b9da5a0e319264ec3132d26
0de2fa7d5040e72f214c917c51252b2a
6862a3634ce144ef8a17f72149c797be
abf439ce8472a080ede1209e6ac23023
83a8d4b7a703b1ab2904a51018c8c43f
C94AA9C9AF53709FD8250CED5B975C20

免责声明及风险提示: