南明离火
移动应用检测平台

ANDROID 静态分析报告

K4

K4 • v1.0.8

本报告由南明离火移动安全分析平台生成

分析日期: 2024-07-15 10:29:38

应用概览

文件名称:	62b6775bcae8c81a106636a1de921854_40e774245b985897a2579a45a6b9b3fb_8.apk
文件大小:	23.71MB
应用名称:	K4
软件包名:	com.leon.androidserialportassistant
主活动:	k.chjc.hengda.com.hd_kfour_chjc_k.ac.MainActivity
版本号:	1.0.8
最小SDK:	17
目标SDK:	25
加固信息:	未加壳
应用程序安全分数:	29/100 (重大风险)
跟踪器检测:	1/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	62b6775bcae8c81a106636a1de921854
SHA1:	35db48ba28dd8db3f3619869d[illegible]f8deb8c
SHA256:	1e1c54976f01577507d82e9[illegible]1519a62483a0d062d

分析结果严重性分布

高危	中危	信息	安全	关注
15	12	1	2	1

四大组件导出状态统计

Activity组件：21个，其中export的有：0个
Service组件：7个，其中export的有：6个
Receiver组件：1个，其中export的有：1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: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2020-11-06 07:39:36+00:00
有效期至: 2050-10-30 07:39:36+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha1
证书MD5: 1ab3fe0208b927ae70819cefebe37b10
证书SHA1: 777f64631ffbe742d3fec29cbd7df7ad2a82f260
证书SHA256: ef806e8d68255c366af3ff028bc410c4fada3697b32db3d1eae1e317bb7f272e
证书SHA512:
6555ba936f3a294c6ec472c04029d605302c0bff8d5ec922566e9b71f5fdfd1681572a62d511bf7f83d95c29e964587dd9eaf7c9d46829fa1d60c781293606d1

公钥算法: rsa
密钥长度: 2048
指纹: af0e280a311af3990d0f3e7690a413ff5e053b5a720166e5a13b3b5af26e6303
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
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.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.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

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.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
com.hengda.smart.helper.cd.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
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.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **1** | 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
应用程序使用了调试证书进行签名	高危	应用程序使用了调试证书进行签名。生产环境的应用程序不能使用调试证书发布。

Manifest 配置安全分析

高危: **13** | 警告: **3** | 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 4.2-4.2.2, [minSdk=17]	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	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	Activity (k.chjc.hengda.com.hd_kfour_chjc_k.ac.MainActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
5	Activity （k.chjc.hengda.com.hd_kfour_chjc_k.ac.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 (25) 更新到 28 或更高版本以在平台级别修复此问题。
6	Service (k.chjc.hengda.com.hd_kfour_chjc_k.statusbar.HDStatusBar) 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。
7	Activity (k.chjc.hengda.com.hd_kfour_chjc_k.ac.NowTaskActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
8	Activity （k.chjc.hengda.com.hd_kfour_chjc_k.ac.NowTaskActivity） 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 (25) 更新到 28 或更高版本以在平台级别修复此问题。
9	Service (k.chjc.hengda.com.hd_kfour_chjc_k.service.MessageService) 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。
10	Service (k.chjc.hengda.com.hd_kfour_chjc_k.service.LocationService) 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。
11	Activity (k.chjc.hengda.com.hd_kfour_chjc_k.ac.HD_PushMsgActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
12	Activity （k.chjc.hengda.com.hd_kfour_chjc_k.ac.HD_PushMsgActivity） 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 (25) 更新到 28 或更高版本以在平台级别修复此问题。

13	Activity (k.chjc.hengda.com.hd_kfour_chjc_k.ac.HD_CancleTaskActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
14	Activity （k.chjc.hengda.com.hd_kfour_chjc_k.ac.HD_CancleTaskActivity） 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 (25) 更新到 28 或更高版本以在平台级别修复此问题。
15	Activity (k.chjc.hengda.com.hd_kfour_chjc_k.ac.HD_PushTaskActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
16	Activity （k.chjc.hengda.com.hd_kfour_chjc_k.ac.HD_PushTaskActivity） 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 (25) 更新到 28 或更高版本以在平台级别修复此问题。
17	Activity (k.chjc.hengda.com.hd_kfour_chjc_k.ac.HD_PushTimerTaskActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
18	Activity （k.chjc.hengda.com.hd_kfour_chjc_k.ac.HD_PushTimerTaskActivity） 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 (25) 更新到 28 或更高版本以在平台级别修复此问题。
19	Service (k.chjc.hengda.com.hd_kfour_chjc_k.service.RecorderService) 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	Service (k.chjc.hengda.com.hd_kfour_chjc_k.service.HoloadRecordFileService) 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。
21	Broadcast Receiver (k.chjc.hengda.com.hd_kfour_chjc_k.bd.WifiReceiver) 未被保护。 存在一个 intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
22	Service (k.chjc.hengda.com.hd_kfour_chjc_k.service.UpNoService) 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。

代码安全漏洞检测

高危: **1** | 警告: **4** | 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
3	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
4	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	升级会员：解锁高级权限
5	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
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	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
8	IP地址泄露	信息	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-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	armeabi/libserial_port.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	10/30	android.permission.RECORD_AUDIO android.permission.WRITE_SETTINGS android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.ACCESS_FINE_LOCATION android.permission.SYSTEM_ALERT_WINDOW android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.VIBRATE

本报告由南明离火移动安全分析平台生成

其它常用权限	9/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.INTERNET android.permission.READ_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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
com.thoughtworks.xstream	安全	否	No Geolocation information available.
jjxt.gzcjc.com.cn	安全	是	**IP地址:** 183.62.245.167 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://com.thoughtworks.xstream/xstream.source/feature	com/thoughtworks/xstream/io/xml/TraxSource.java
• 183.62.245.167 • https://jjxt.gzcjc.com.cn/api/	k/chjc/hengda/com/hd_kfour_chjc_k/config/ConfigPath.java
• http://com.thoughtworks.xstream/sax/property/configured-xstream • http://com.thoughtworks.xstream/sax/property/api.rce-object-list	com/thoughtworks/xstream/io/xml/SaxWriter.java
• http://com.thoughtworks.xstream/sax/property/source-object-list • http://com.thoughtworks.xstream/xstream.source/feature • http://rqd.uu.qq.com/rqd/sync • https://jjxt.gzcjc.com.cn/api/ • 183.62.245.167 • http://com.thoughtworks.xstream/sax/property/configured-xstream	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

邮箱地址敏感信息提取

EMAIL	源码文件
null@null.xml	com/thoughtworks/xstream/persistence/FilePersistenceStrategy.java
null@null.xml	自研引擎-S

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

敏感凭证泄露检测

可能的密钥
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

免责声明及风险提示: