南明离火
移动应用检测平台

ANDROID 静态分析报告

玖健 • v1.1.1

分析日期: 2024-05-03 14:31:41

应用概览

文件名称:	jiujian_1_1_1.apk
文件大小:	2.95MB
应用名称:	玖健
软件包名:	com.jiujian.org
主活动:	com.uzmap.pkg.LauncherUI
版本号:	1.1.1
最小SDK:	15
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	45/100 (中风险)
杀软检测:	AI评估：安全
MD5:	a3fbee0802deee9fb01a9566cf9dcbad
SHA1:	ae69e828650ba62ef5e301fe32d50f0949e595dc
SHA256:	64958b6ba10f886dbeecd3c0[illegible]ce67d1170a87273[illegible]c2c873a71c32f93

分析结果严重性分布

高危	中危	信息	安全	关注
6	10	11	3	1

四大组件导出状态统计

Activity组件：3个，其中export的有：0个
Service组件：1个，其中export的有：0个
Receiver组件：1个，其中export的有：0个
Provider组件：2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=zh, ST=Beijing, L=Beijing, O=test, OU=test, CN=www.ctbri.com
签名算法: rsassa_pkcs1v15
有效期自: 2023-08-15 12:15:19+00:00
有效期至: 2123-07-22 12:15:19+00:00
发行人: C=zh, ST=Beijing, L=Beijing, O=test, OU=test, CN=www.ctbri.com
序列号: 0x5796ab5
哈希算法: sha1
证书MD5: ac09844ebf254fa157222bca09fe56a0
证书SHA1: 1b12a03a0fee94cb0de2b2715380900181c7059b
证书SHA256: 7dc65c3456e5e52df34b9e7c265b6f81d5a8a679c6356e3bb72daf23f528b72c
证书SHA512:
a1d640c085646772623565e4d832e39736c727b7587fdbffc022d98ded6ead15bc1f72ae17429f41f31d4a07ef5a1e5cc3d8204f8267fc4200d11dc0d6f90786

公钥算法: rsa
密钥长度: 1024
指纹: c6336ddadeff86d3d7ff9c8a3c7a1d7e594546469c13702d400fc1eb0fafd2c8
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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
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_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.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.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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。

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: **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: **2** | 警告: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 4.0.3-4.0.4, [minSdk=15]	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	Activity (com.uzmap.pkg.LauncherUI) is vulnerable to StrandHogg 2.0	高危	已发现活动容易受 StrandHogg 2.0 任务劫持漏洞的风险。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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
4	Activity (com.uzmap.pkg.EntranceActivity) 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。

代码安全漏洞检测

高危: **4** | 警告: **7** | 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
2	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
3	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

本报告由南明离火移动安全分析平台生成

4	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
5	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
6	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
7	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
8	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
9	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。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	升级会员：解锁高级权限
10	该文件是World Readable。任何应用程序都可以读取文件	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
11	应用程序使用SQLite数据库执行原始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

12	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
13	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
14	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

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/libsec.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	5/30	android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.CAMERA android.permission.CALL_PHONE android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	6/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE

常用: 已知恶意软件广泛使用的权限。

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
d.app3c.cn	安全	否	No Geolocation information available.
s.app3c.com	安全	否	No Geolocation information available.

www.ccil.org	安全	否	**IP地址:** 142.250.207.19 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
iuap-yonbuilder-mamservice.yyuap.com	安全	是	**IP地址:** 59.110.247.93 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397103 **查看:** 高德地图
p.app3c.cn	安全	否	No Geolocation information available.
as.app3c.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://www.ccil.org/~cowan/tagsoup/properties/schema	com/deepe/c/i/o.java
• https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	com/deepe/c/l/a.java
• https://iuap-yonbuilder-mamservice.yyuap.com/iuap-yonbuilder-mobile/v2 • https://d.app3c.cn • https://s.app3c.com • https://p.app3c.cn • https://as.app3c.com	compile/Properties.java
• https://d.app3c.cn • http://www.ccil.org/~cowan/tagsoup/properties/schema • https://p.app3c.cn • https://s.app3c.com • https://as.app3c.com • https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection • https://iuap-yonbuilder-mamservice.yyuap.com/iuap-yonbuilder-mobile/v2	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。

敏感凭证泄露检测

可能的密钥
aHR0cHM6Ly93d3cuZ29vZ2xlLWFuYWx5dGljcy5jb20vY29sbGVjdA==

aHR0cHM6Ly93d3cuZ29vZ2xlLWFuYWx5dGljcy5jb20vYmF0Y2g=
YW5kcm9pZC50ZWxlcGhvbnkuU21zTWFuYWdlcg==
y2n9vbBttkeZ516MWLPG0nYZOrQ0VCec+t0dBPA/5NfVAAy7
ZGlzdC9iYXNlL2FwaWJhc2UuanM=
62587239-AD3C-8190-47B4-37DE080D7E9D
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

免责声明及风险提示: