南明离火
移动应用检测平台

ANDROID 静态分析报告

萝莉社 • v2.4.81

分析日期: 2024-07-16 13:47:44

应用概览

文件名称:	萝莉社.apk
文件大小:	9.35MB
应用名称:	萝莉社
软件包名:	newabv.dmm.singiwkk.zkzhyw1
主活动:	com.hqzx.hqzxdetail.activity.SplashActivity
版本号:	2.4.8.1
最小SDK:	22
目标SDK:	31
加固信息:	未加壳
应用程序安全分数:	40/100 (中风险)
跟踪器检测:	1/432
杀软检测:	5 个杀毒软件报毒
MD5:	d574e1b45a1fa681e55412d988404f67
SHA1:	27b3e5e585723eca9ed518a[illegible]c2b439e8cc1436
SHA256:	c4f72bdcbd8d82b6653f[illegible]78f6c7504b86e0594de[illegible]2e702fa591a97f6596

分析结果严重性分布

高危	中危	信息	安全	关注
5	13	2	1	3

四大组件导出状态统计

Activity组件：19个，其中export的有： 0个
Service组件：3个，其中export的有： 0个
Receiver组件：1个，其中export的有： 1个
Provider组件：4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: True
v4 签名: False
主题: C=beijing, ST=beijing, L=beijing, O=yz1721075206059, OU=jp1721075206059, CN=qdir
签名算法: rsassa_pkcs1v15
有效期自: 2024-07-15 20:26:53+00:00
有效期至: 2074-07-03 20:26:53+00:00
发行人: C=beijing, ST=beijing, L=beijing, O=yz1721075206059, OU=jp1721075206059, CN=qdir
序列号: 0x5eeb9fa0
哈希算法: sha512
证书MD5: ece75d194abd275623cdbe95ebb18d5b
证书SHA1: 251152a48f5ca535c19ddbb48cff4c173be892e5
证书SHA256: 792899ce7d5d63c26590c3082e1a66d4eed13c61b03e8c4465e890ad19c21593
证书SHA512:
87c9e4a6d1345af287dbbfe08f6b99ebbc25ad772bff1ef3360a7be68f41be0e107ac53f77471c5d25210948f3e583045e4275d48ff4ba85c401acbd72c14e58

公钥算法: rsa
密钥长度: 4096
指纹: 3ea45084822a995f0f86197f0005684f76baf59fbd55d1028e104384c449a3b3
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。
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.READ_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.hqzx.hqzxdetail.activity.SplashActivity	Schemes: kni70m://,

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

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.1-5.1.1, [minSdk=22]	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_https_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	Broadcast Receiver (com.liciclaim.android.download.SystemDownloadReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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: **4** | 警告: **9** | 信息: **2** | 安全: **1** | 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	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
3	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
4	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
5	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
6	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
7	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
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	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
10	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

11	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
12	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
13	已启用远程WebView调试	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
14	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	高危	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-2	升级会员：解锁高级权限
15	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
16	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	3/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.CALL_PHONE

本报告由南明离火移动安全分析平台生成

其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_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
yingshi.shop	安全	是	**IP地址:** 61.160.148.90 **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
ulogs.umengcloud.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777992 **查看:** 高德地图
aria.laoyuyu.me	安全	是	**IP地址:** 118.24.25.24 **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
llsapi.eydni.com	安全	否	**IP地址:** 154.84.24.238 **国家:** 马来西亚 **地区:** 柔佛 **城市:** 柔佛新山 **纬度:** 1.465653 **经度:** 103.757721 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://aria.laoyuyu.me/aria_doc/api/use_broadcast.html	自研引擎-A
• 2.4.8.1	自研引擎-M
• 2.4.8.1	com/hqzx/hqzxdetail/BuildConfig.java

• 8.8.8.8	org/minidns/DnsClient.java
• https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java
• 127.0.0.1	com/snail/antifake/deviceid/IpScanner.java
• http://%s:%d/%s	com/danikula/videocache/Pinger.java
• 1.9.2.6	com/arialyy/aria/http/upload/HttpUThreadTaskAdapter.java
• https://github.com/arialyy/aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Option.java
• https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
• http://127.0.0.1:8080	com/hqzx/hqzxdetail/activity/FullVideoActivity.java
• 127.0.0.1	fi/iki/elonen/NanoHTTPD.java
• https://llsapi.eydni.com	com/hqzx/hqzxdetail/app/App.java
• https://yingshi.shop/	com/hqzx/hqzxdetail/http/Config.java
• http://%s:%d/%s • 127.0.0.1	com/danikula/videocache/HttpProxyCacheServer.java
• https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java

• https://tbs.imtt.qq.com/plugin/debugplugin_v2.tbs • https://pms.mb.qq.com/rsp204 • 8.8.8.8 • https://debugtbs.qq.com • 127.0.0.1 • https://aria.laoyuyu.me/aria_doc/create/any_java.html • 10.0.0.172 • file:unexpect • https://debugtbs.qq.com?10000 • 1.9.2.6 • http://127.0.0.1:8080 • 2.4.8.1 • https://cfg.imtt.qq.com/tbs?v=2&mk= • www.qq.com • https://yingshi.shop/ • https://github.com/arialyy/aria/issues/597 • http://%s:%d/%s • https://llsapi.eydni.com • https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html • https://mdc.html5.qq.com/mh?channel_id=50079&u= • https://ulogs.umengcloud.com • https://debugx5.qq.com • https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
AntiFakerAndroidChecker	happylishang	Android 模拟器检测，检测 Android 模拟器，作为可信 DeviceID，应对防刷需求等。
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。
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 App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

邮箱地址敏感信息提取

EMAIL	源码文件
x5tbs@tencent.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
openinstall统计的=> "com.openinstall.APP_KEY" : "kni70m"
8D91E471E0989CDA27DF505A453F2B7635294F2DDF23E3B122ACC99C9E9F1E14
162868615546106446534825224972501099617764973866649250057266444446153280773974453602977161065924104934399403805354129041996887056318385686578091637657155037251347695787084332273120879361960335192976650756927217125865840030576429696147778001233984421619267530978084631948434496468785021389956803104620471232008587410372435192296507420228042196341907342725062200186579201369020143938340926487855145488763700289254055576617593999013788169116831224740387349125354256705332378156761348407395656109637964274018557230266870736004454610907362400302479060950538754912258796566400527339409054403629739010411098931881910665319991749 3
AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25BFF55296C3A545E3872760AB7
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
659eab6595b14f599d146582
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
3617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
4FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A1394D1898C296

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。