南明离火
移动应用检测平台

ANDROID 静态分析报告

黑料网 • v1.0.0

分析日期: 2024-03-01 08:58:23

应用概览

文件名称:	hlwapp_1.0.0_240225_4.apk
文件大小:	38.76MB
应用名称:	黑料网
软件包名:	us.yqhwn.rvvwhl
主活动:	com.mater.ct.mater.MainActivity
版本号:	1.0.0
最小SDK:	21
目标SDK:	31
加固信息:	Flutter/Dart 加固
应用程序安全分数:	52/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	1749823da6ae04e1674f8c34ce01545d
SHA1:	736422be36a4be7b06b8caa2174ee828bba454d8
SHA256:	3ee32e88580cea5545dfe5a368f40f22f7b8ee3776ba867016e0629c6d97291e4

分析结果严重性分布

高危	中危	信息	安全	关注
1	8	2	1	0

四大组件导出状态统计

Activity组件：2个，其中export的有：0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

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: 2022-11-03 10:16:02+00:00
有效期至: 2052-10-26 10:16:02+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha1
证书MD5: 7d8a2c0d2493e5d6d85c3865d0918482
证书SHA1: 7682ef35f017d1b3d352557971c295a6885fae4c
证书SHA256: 7b86e6199d7c910d075153a0fe61cf241a4b390dd5f4dd0a74381dab7cf42b6f
证书SHA512:
5d1a8d09f651ee318f3411e559df66a5439dfea5538839f3bc527c6fa3a0671d1326e28949e56f2766e9f716b69ff5ecb1298370c4bb59b7701a43ef4744178b

公钥算法: rsa
密钥长度: 2048
指纹: a715c81d7c87ff29afca669875aed119aeed1a6f489b5d567f6e4c3922f04e1f
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.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.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.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.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.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.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.DOWNLOAD_WITHOUT_NOTIFICATION	普通	后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。
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.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.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。

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
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。
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: **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 5.0-5.0.2, [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	应用程序具有网络安全配置 [android:networkSecurityConfig=0x7f0c0002]	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。
3	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志[android:allowBackup]应该设置为false。默认情况下它被设置为true，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。

代码安全漏洞检测

高危: **0** | 警告: **4** | 信息: **2** | 安全: **0** | 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

3	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
4	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
5	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
6	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	5/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE 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

data.flurry.com	安全	否	**IP地址:** 209.73.190.11 **国家:** United States of America **地区:** New York **城市:** New York City **纬度:** 40.731323 **经度:** -73.990089 **查看:** Google 地图
exoplayer.dev	安全	否	**IP地址:** 185.199.110.153 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
aomedia.org	安全	否	**IP地址:** 185.199.111.153 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
dashif.org	安全	否	**IP地址:** 185.199.110.153 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
schemas.microsoft.com	安全	否	**IP地址:** 13.107.213.74 **国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图
proton.flurry.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://ns.adobe.com/xap/1.0/	e/d/a/a.java
• https://data.flurry.com/pcr.do	f/d/b/a0.java
• https://data.flurry.com/aap.do • http://data.flurry.com/aap.do	f/d/b/k0.java
• https://proton.flurry.com/sdk/v1/config	f/d/b/s.java
• https://exoplayer.dev/issues/player-accessed-on-wrong-thread	f/e/a/a/e2.java
• https://exoplayer.dev/issues/cleartext-not-permitted	f/e/a/a/e4/d0.java

• http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	f/e/a/a/w3/l0.java
• http://ns.adobe.com/xap/1.0/	f/e/a/a/x3/m0/a.java
• https://aomedia.org/emsg/ID3 • https://developer.apple.com/streaming/emsg-id3	f/e/a/a/z3/j/a.java
• https://developer.android.com/guide/topics/permissions/overview	i/a/c/d/e.java
• https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/d/t.java
• http://dashif.org/guidelines/last-segment-number • https://data.flurry.com/aap.do • https://data.flurry.com/pcr.do • https://aomedia.org/emsg/ID3 • data:cs:AudioPurposeCS:2007 • https://exoplayer.dev/issues/player-accessed-on-wrong-thread • https://proton.flurry.com/sdk/v1/config • http://data.flurry.com/aap.do • https://developer.apple.com/streaming/emsg-id3 • https://exoplayer.dev/issues/cleartext-not-permitted • http://dashif.org/guidelines/trickmode • http://ns.adobe.com/xap/1.0/ • https://developer.android.com/guide/topics/permissions/overview • http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense • https://developer.android.com/reference/javax/net/ssl/SSLSocket	自研引擎分析结果

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
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 架构清晰、简单易用等优势。
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
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

---

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端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患。

本报告由南明离火移动安全分析平台生成