南明离火
移动应用检测平台

ANDROID 静态分析报告

好莱污 • v1.0.0

分析日期: 2024-03-18 08:24:26

应用概览

文件名称:	20240208-222123.apk
文件大小:	22.99MB
应用名称:	好莱污
软件包名:	com.flutter3.chlw.fb0eem
主活动:	com.media.flutter.flutter2_frame.MainActivity
版本号:	1.0.0
最小SDK:	21
目标SDK:	33
加固信息:	Flutter/Dart 加固
应用程序安全分数:	43/100 (中风险)
杀软检测:	AI评估：安全
MD5:	9d05834c110b08c5bf6379fb1053c4fc
SHA1:	5418b0a608052443fccf726002cd0645d3a53b72
SHA256:	0db0db7118f85b76027612185eb7f3d7f191bed94d1048e062eee7096e0d08e8

分析结果严重性分布

高危	中危	信息	安全	关注
3	8	12	1	1

四大组件导出状态统计

Activity组件：4个，其中export的有：0个
Service组件：1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: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2024-01-24 20:00:02+00:00
有效期至: 2051-06-11 20:00:02+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x23b5d2ca
哈希算法: sha256
证书MD5: 5d09057d14a014e1748a719d093a4b42
证书SHA1: ba95d85bbc3889426f693a482f27f73bc18e9363
证书SHA256: 460d10e5fe3f6e5d73701191e0a94b68cc8f1eedd20739c23a7b7c28c4a97773
证书SHA512:
fbb7f4727388e895ce164ed29ef1aa896a4c014b61836c369297ec57d92defcef69e41615fc9ea743ac5b764ea9813232e963f1a367a39[illegible]6f1117e92b59e

公钥算法: rsa
密钥长度: 2048
指纹: c5aefd982a211ab8c0b4010854f10d5bbfb2f6a63406333fce59e5c8ad347a1b
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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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。
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。

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
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。

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=0x7f110001]	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调试的用户从设备拷贝复制应用程序数据。

代码安全漏洞检测

高危: **2** | 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
3	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

4	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
5	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
6	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
7	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
8	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	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.CAMERA android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE
其它常用权限	6/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE

常用: 已知恶意软件经常滥用的权限。

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
exoplayer.dev	安全	否	**IP地址:** 185.199.109.153 **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:** 185.199.108.153 **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:** 47.682809 **经度:** -122.120903 **查看:** Google 地图
dashif.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
app.mi.com	安全	是	**IP地址:** 118.26.252.203 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	b1/l0.java
• http://dashif.org/guidelines/last-segment-number • data:cs:AudioPurposeCS:2007 • http://dashif.org/guidelines/trickmode	d2/d.java
• https://plus.google.com/	e3/h0.java
• http://ns.adobe.com/xap/1.0/	h1/a.java
• https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/c.java

• https://aomedia.org/emsg/ID3 • https://developer.apple.com/streaming/emsg-id3	r1/a.java
• https://exoplayer.dev/issues/cleartext-not-permitted	t2/z.java
• https://a.app.qq.com/o/simple.jsp?pkgname=	v0/b.java
• https://app.mi.com/details?id= • https://app.mi.com	v0/c.java
• https://exoplayer.dev/issues/player-accessed-on-wrong-thread	x0/b1.java
• http://undefined/	z7/d.java
• http://ns.adobe.com/xap/1.0/ • https://developer.android.com/guide/topics/permissions/overview • http://undefined/ • http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense • http://dashif.org/guidelines/last-segment-number • https://exoplayer.dev/issues/cleartext-not-permitted • data:cs:AudioPurposeCS:2007 • https://app.mi.com • https://a.app.qq.com/o/simple.jsp?pkgname= • https://app.mi.com/details?id= • http://dashif.org/guidelines/trickmode • https://developer.apple.com/streaming/emsg-id3 • https://aomedia.org/emsg/ID3 • https://exoplayer.dev/issues/player-accessed-on-wrong-thread • https://plus.google.com/	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。
RUpgrade	rhymelph	Android 和iOS 热升级应用插件。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。

邮箱地址敏感信息提取

EMAIL	源码文件
u0013android@android.com0 u0013android@android.com	a3/s.java
android@android.com0	自研引擎分析结果

敏感凭证泄露检测

可能的密钥

9a04f079-9840-4286-ab92-e65be0885f95
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
e2719d58-a985-b3c9-781a-b030af78d30e
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy

免责声明及风险提示: