南明离火
移动应用检测平台

# ANDROID 静态分析报告

草玫影视 • v1.3



分析日期: 2024-03-24 11:39:25

# 应用概览

| | |
|---|---|
| 文件名称: | 草玫影视.apk |
| 文件大小: | 6.51MB |
| 应用名称: | 草玫影视 |
| 软件包名: | com.cpsmyilsuoao.cpsmemaetynv |
| 主活动: | com.e4a.runtime.android.StartActivity |
| 版本号: | 1.8 |
| 最小SDK: | 20 |
| 目标SDK: | 29 |
| 加固信息: | 未加壳 |
| 应用程序安全分数: | 39/100 (高风险) |
| 跟踪器检测: | 1/432 |
| 杀软检测: | 11 个杀毒软件报毒 |
| MD5: | bad0623fff69e7950d7e9b0ad6e0dd34 |
| SHA1: | fc3e8a806ff03bc2f7bd835310b6879daa485eb4 |
| SHA256: | c667c263145e1e66b86caeeca7c201d35ea4c7a8318238838fa7cfb234018514 |

# 分析结果严重性分布

| 高危 | 中危 | 信息 | 安全 | 关注 |
|---|---|---|---|---|
| 3 | 11 | 1 | 0 | 4 |

# 四大组件导出状态统计

| |
|---|
| Activity组件：2个，其中export的有：1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：1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=XT, ST=VSOEIU, L=XTG15Z, O=LHC9AJ, OU=4EMWQI, CN=T5QLVB
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-09 18:35:54+00:00
有效期至: 2297-08-24 18:35:54+00:00
发行人: C=XT, ST=VSOEIU, L=XTG15Z, O=LHC9AJ, OU=4EMWQI, CN=T5QLVB
序列号: 0xdf34e59
哈希算法: sha256
证书MD5: 6fdb385f2fc014a6e04269511b8c6797
证书SHA1: 71b9eeed580d43b4133b9c97bd117f0118119db8
证书SHA256: a112eeac9daf808b88c37e5e5dade80f056d7a592871b2865e043921a662df2a
证书SHA512:
74ddc23162de6995544614bfed0468a039fc4862d1af8a8b9b4a3164e6a739686f1296d628ba0dccb9291aaa53d6a6b1f3f0d72b31901cdd8fc1b3a23a38710

公钥算法: rsa
密钥长度: 2048
指纹: 8830bb923882496f73e1a228c639c51478c0e91821c6f0429987483307c7736b
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 |
| --- | --- | --- | --- |
| com.android.launcher.permission.READ_SETTINGS | 危险 | 读取桌面快捷方式 | 这种权限的作用是允许应用读取桌面快捷方式的设置。 |
| android.permission.CHANGE_CONFIGURATION | 危险 | 改变UI设置 | 允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。 |
| 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.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.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.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.SYSTEM_OVERLAY_WINDOW | 未知 | 未知权限 | 来自 android 引用的未知权限。 |
| 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.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.GET_TASKS | 危险 | 检索当前运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。 |
| 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.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.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_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。 |
| com.android.launcher.permission.INSTALL_SHORTCUT | 签名 | 创建快捷方式 | 这个权限是允许应用程序创建桌面快捷方式。 |

## 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 |
| 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，那么它就会易受到安卓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: **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<br>Android 4.4W-4.4W.2, [minSdk=20] | 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 | 应用程序数据存在被泄露的风险<br>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。 |
| 3 | Activity (com.efa.untime.android.MainActivity) 未被保护。<br>存在一个 intent-filter。 | 警告 | 发现 Activity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Activity是显式导出的。 |

## 代码安全漏洞检测

高危: **3** | 警告: **5** | 信息: **1** | 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<br>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<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 升级会员：解锁高级权限 |
| 3 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | 升级会员：解锁高级权限 |
| 4 | 使用弱加密算法 | 高危 | CWE: CWE-327: 使用已被攻破或存在风险的密码学算法<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 升级会员：解锁高级权限 |
| 5 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-3 | 升级会员：解锁高级权限 |
| 6 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 升级会员：解锁高级权限 |
| 7 | 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<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-RESILIENCE-2 | 升级会员：解锁高级权限 |
| 8 | IP地址泄露 | 警告 | CWE: CWE-200: 信息泄露<br>OWASP MASVS: MSTG-CODE-2 | 升级会员：解锁高级权限 |
| 9 | 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'）<br>OWASP Top 10: M7: Client Code Quality | 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.VIBRATE<br>android.permission.SYSTEM_ALERT_WINDOW<br>android.permission.REQUEST_INSTALL_PACKAGES<br>android.permission.GET_TASKS<br>android.permission.WAKE_LOCK<br>android.permission.READ_PHONE_STATE |
| 其它常用权限 | 7/46 | android.permission.FOREGROUND_SERVICE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.INTERNET<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.READ_EXTERNAL_STORAGE<br>com.android.launcher.permission.INSTALL_SHORTCUT |

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 |
| --- | --- | --- | --- |
| log.umsns.com | 安全 | 是 | **IP地址:** 59.82.60.43<br>**国家:** China<br>**地区:** Beijing<br>**城市:** Beijing<br>**纬度:** 39.907501<br>**经度:** 116.397232<br>**查看:** 高德地图 |
| oc.umeng.co | 安全 | 否 | No Geolocation information available. |
| www.eruyi.cn | 安全 | 否 | **IP地址:** 39.109.112.217<br>**国家:** Hong Kong<br>**地区:** Hong Kong<br>**城市:** Hong Kong<br>**纬度:** 22.285521<br>**经度:** 114.157692<br>**查看:** Google 地图 |
| www.123cha.com | 安全 | 是 | **IP地址:** 58.220.63.20<br>**国家:** China<br>**地区:** Jiangsu<br>**城市:** Yangzhou<br>**纬度:** 32.397221<br>**经度:** 119.435829<br>**查看:** 高德地图 |
| bbs.e4asof[illegible].com | 安全 | 是 | **IP地址:** 43.248.189.45<br>**国家:** China<br>**地区:** Jiangsu<br>**城市:** Suqian<br>**纬度:** 33.933334<br>**经度:** 118.283333<br>**查看:** 高德地图 |

| | | | |
|---|---|---|---|
| alog.umeng.co | 安全 | 否 | No Geolocation information available. |
| bbs.e4asoft.compath | 安全 | 否 | No Geolocation information available. |

## URL 链接安全分析

| URL信息 | 源码文件 |
|---|---|
| • www.eruyi.cn | com/cpsmyilsuoao/cpsmemaetynv/C0003.java |
| • www.eruyi.cn | com/cpsmyilsuoao/cpsmemaetynv/C0005.java |
| • www.eruyi.cn | com/cpsmyilsuoao/cpsmemaetynv/video.java |
| • http://bbs.e4asoft.com;path=/<br>• http://www.123cha.com/<br>• http://api.fanyi.baidu.com/api/trans/vip/translate?q= | com/e4a/runtime/C0055.java |
| • http://bbs.e4asoft.com/openapi_unsafe.php | com/e4a/runtime/MySQL.java |
| • www.eruyi.cn | com/e4a/runtime/components/impl/android/b008/Impl.java |
| • 10.0.0.172 | u/aly/r.java |
| • 10.0.0.172<br>• http://oc.umeng.co/check_config_update<br>• www.eruyi.cn<br>• http://alog.umeng.co/app_logs<br>• http://bbs.e4asoft.com/openapi_unsafe.php<br>• http://bbs.e4asoft.com;path=/<br>• 5.2.4.1<br>• http://api.fanyi.baidu.com/api/trans/vip/translate?q=<br>• http://log.umsns.com/<br>• http://log.umsns.com/share/api/<br>• http://www.123cha.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 |
|---|---|---|
| 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。 |

## 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 |
| --- |
| 6E4DDD42F7F02C5B847E6C8AFA7292A1414828F9CFA49D1B651839FF87C56312A87CBA3710A7 |
| 6E4DDD42F7F02C5B847E6C8AFA7292A141482AF9CFA49D1B651839FF87C56341E767FC37 |
| 6E4DDD42F7F02C5B847E6C8AFA7292A1414829F9CFA49D1B651839FF87C56341E767FC37 |
| 6255560c0059ce2bad32aaf5 |

## 免责声明及风险提示: