南明离火
移动应用检测平台

ANDROID 静态分析报告

草莓影盒V03201737 • v1.8

分析日期: 2024-05-27 20:54:46

应用概览

文件名称:	test2.apk
文件大小:	5.43MB
应用名称:	草莓影盒V03201737
软件包名:	com.cpsmpzzzangf.cpsmiwvrxnjh
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:	44/100 (中风险)
跟踪器检测:	1/432
杀软检测:	20 个杀毒软件报毒
MD5:	29e9bbb51a5b115132177d30f42c7cc5
SHA1:	d29c71cee9d31bbae2f51803[illegible]d1285f8ad
SHA256:	58ea974420de6dc31f1a[illegible]1040c16125050f6a9b[illegible]edacdaa86f283b2b5

分析结果严重性分布

高危	中危	信息	安全	关注
1	8	1	0	3

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=SR, ST=9YVJ5F, L=CADREI, O=QGEW5N, OU=8Y00QE, CN=H96ZVJ
签名算法: rsassa_pkcs1v15
有效期自: 2024-03-20 09:37:26+00:00
有效期至: 2298-01-03 09:37:26+00:00
发行人: C=SR, ST=9YVJ5F, L=CADREI, O=QGEW5N, OU=8Y00QE, CN=H96ZVJ
序列号: 0xcfc8517
哈希算法: sha256
证书MD5: 4e42ee4c80ac674195ff47bb1a2e550a
证书SHA1: 69f11c421d5ce424bc39de1095be4acba9960f1e
证书SHA256: f2ae0d63d921c95e1a31bc79d6d7a5a7a969e9bc817c50312f83784c7ad61efa
证书SHA512:
bba134aeeae3881260fd267d5b7df1e016652fc64677dbe91e879a65f0d78f49091cb531fdc96f265589d9cfc11ebcd684f42db4daef66c34cd8231efd26410c

公钥算法: rsa
密钥长度: 2048
指纹: d7c851bb657043ec2445339bfb00f72089030b55f8ec38c12284969d7a06313c
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

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 4.4W-4.4W.2, [minSdk=20]	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。
3	Activity (com.e4a.runtime.android.mainActivity) 未被保护。 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: **1** | 警告: **4** | 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

本报告由南明离火移动安全分析平台生成

2	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
3	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 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
4	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
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	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

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 android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE
其它常用权限	7/46	android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE 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
bbs.e4asoft.com	安全	是	**IP地址:** 43.248.189.45 **国家:** 中国 **地区:** 江苏 **城市:** 宿迁 **纬度:** 33.933334 **经度:** 118.283333 **查看:** 高德地图
alog.umeng.co	安全	否	No Geolocation information available.
log.umsns.com	安全	是	**IP地址:** 59.82.29.249 **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
oc.umeng.co	安全	否	No Geolocation information available.
bbs.e4asoft.compath	安全	否	No Geolocation information available.
www.123cha.com	安全	是	**IP地址:** 59.82.29.249 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• 10.0.0.172	u/aly/r.java
• 10.0.0.172 • http://log.umsns.com/share/api/ • http://oc.umeng.co/check_config_update • http://alog.umeng.co/app_logs • http://log.umsns.com/ • http://www.123cha.com/ • http://bbs.e4asoft.com;path=/ • http://bbs.e4asoft.com/openapi_unsafe.php • http://api.fanyi.baidu.com/api/trans/vip/translate?q= • 5.2.4.1	自研引擎-S

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
9FABC82B8C1C08354D76B90D227243985007AE64EE87F5FF4C65FF562958D86FBD0D7C19FED8
9FABC82BC509082E0D2FFF13773A0AD0044AF27FA28CF9A44971F95B6D04C465AC
9FABC82B8C1C08354D76B90D2D79578A4A15A864F987E8FF4C65FF562958D83CF2163A19
9FABC82B8C1C08354D76B90D227243985007A964EE87F5FF4C65FF562958D86FBD0D7C19FED8
9FABC82B8C1C08354D76B90D2D79578A4A15AB64F987E8FF4C65FF562958D83CF2163A19
6255560c0059ce2bad32aaf5
9FABC82BC509082E092FFF10793A0ADB064AF87BA28CF9A44971F95B6D04C465AC

免责声明及风险提示: