南明离火
移动应用检测平台

ANDROID 静态分析报告

MaVeCY • v1.0

分析日期: 2024-05-06 13:44:24

应用概览

文件名称:	MaVeCY.apk
文件大小:	5.78MB
应用名称:	MaVeCY
软件包名:	com.my.mavecy2
主活动:	.MainActivity
版本号:	1.0
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	2/432
杀软检测:	5 个杀毒软件报毒
MD5:	3cfbc13357d4b7c1eaf8c1166b3e1534
SHA1:	fd0cc82f22aefe6a78b8219586760[illegible]f99cf449
SHA256:	7e1809d4d18e18b233b4[illegible]14f282dfd3e5272a948[illegible]5d6c06ced4eb406c184

分析结果严重性分布

高危	中等	信息	安全	关注
3	13	1	2	0

四大组件导出状态统计

Activity组件：7个，其中export的有：3个
Service组件：2个，其中export的有：0个
Receiver组件：1个，其中export的有：1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: False
v4 签名: False
主题: C=debugging
签名算法: rsassa_pkcs1v15
有效期自: 2016-09-23 11:57:06+00:00
有效期至: 3015-01-25 11:57:06+00:00
发行人: C=debugging
序列号: 0x333a0b9b
哈希算法: sha256
证书MD5: c13f92d0397da7423a4142bfa9a5873e
证书SHA1: d122d9adc3e5d5ff346b32c0413f5cf3a3cc4658
证书SHA256: 022a1ed9feb0e6c9826df99c58350b7789a71ad51f142f40449f91d58c0278c1
证书SHA512:
f8ac9decdd241b79396dddeb68c9f2d3d1c909bcee3a32f43e286b7ab8211de05d8f1c9e3e8328c85fd4c948e7edeb2b90c45a09[illegible]9050d40433d5b2a90c6e4d

公钥算法: rsa
密钥长度: 2048
指纹: a09cf4ea0b0d8f9b0db4f186cc988aa8b975f458a68003aea0a6af81570420ca
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.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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.TV_INPUT_HARDWARE	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_PEOPLE_DATA	未知	未知权限	来自 android 引用的未知权限。
android.permission.REQUEST_COMPANION_USE_DATA_IN_BACKGROUND	普通	允许配套应用程序在后台使用数据	允许配套应用在后台使用数据。
android.permission.ACCESS_NETWORK_CONDITIONS	未知	未知权限	来自 android 引用的未知权限。

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: **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 Android 5.0-5.0.2, [minSdk=21]	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	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过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。
4	Broadcast Receiver (com.startapp.sdk.adsbase.remoteconfig.BootCompleteListener) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此计算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Broadcast Receiver是显式导出的。

代码安全漏洞检测

高危: **3** | 警告: **8** | 信息: **1** | 安全: **2** | 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	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
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 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
4	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

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	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
7	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
8	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
9	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
10	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
11	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	升级会员：解锁高级权限
12	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
13	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
14	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN

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
support.startapp.com	安全	否	**IP地址:** 150.136.126.70 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.03947 **经度:** -77.491306 **查看:** Google 地图
daneden.me	安全	否	**IP地址:** 76.76.21.61 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 核桃 **纬度:** 34.015400 **经度:** -117.858223 **查看:** Google 地图
opensource.org	安全	否	**IP地址:** 199.16.173.137 **国家:** 美利坚合众国 **地区:** 得克萨斯州 **城市:** 圣安东尼奥 **纬度:** 29.425426 **经度:** -98.489349 **查看:** Google 地图
geoip.api.c0nnect[redacted]ts.com	安全	否	**IP地址:** 52.211.224.166 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
awsdus.api.p3insight.de	安全	否	No Geolocation information available.
req.startappservice.com	安全	否	**IP地址:** 168.138.175.122 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图

imp.startappservice.com	安全	否	**IP地址:** 168.138.188.189 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
adsmetadata.startappservice.com	安全	否	**IP地址:** 168.138.188.189 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
info.startappservice.com	安全	否	**IP地址:** 152.195.62.69 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 33.972069 **经度:** -118.430313 **查看:** Google 地图
lh6.ggpht.com	安全	否	**IP地址:** 142.251.222.33 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
d1byvlfiet2h9q.cloudfront.net	安全	否	No Geolocation information available.
ul.api.c0nnectthed0ts.com	安全	否	**IP地址:** 34.255.85.247 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
d2to8y50b3n6dq.cloudfront.net	安全	否	No Geolocation information available.
geoip.api.p3insight.de	安全	否	No Geolocation information available.
www.com.startapp.com	安全	否	No Geolocation information available.
mavecy.site	安全	否	**IP地址:** 66.29.146.222 **国家:** 美利坚合众国 **地区:** 佐治亚州 **城市:** 亚特兰大 **纬度:** 33.727291 **经度:** -84.425377 **查看:** Google 地图
infoevent.startappservice.com	安全	否	**IP地址:** 168.138.175.122 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://mavecy.site/	com/my/mavecy2/LuanchActivity.java
• https://mavecy.site/	com/my/mavecy2/MainActivity.java
• 10.0.2.15	com/startapp/a/a/a.java
• https://awsdus.api.p3insight.de/isupload/upload_check_lumen.php • https://ul.api.c0nnectthed0ts.com/ul/v3/ • https://d2to8y50b3n6dq.cloudfront.net/truststores/ • https://geoip.api.c0nnectthed0ts.com/geoip/	com/startapp/networkTest/a.java
• 127.0.0.1	com/startapp/networkTest/d/a/b.java
• https://d2to8y50b3n6dq.cloudfront.net/truststores/ • https://geoip.api.c0nnectthed0ts.com/geoip/	com/startapp/networkTest/startapp/NetworkTester.java
• https://daneden.me/animate • https://lh6.ggpht.com/vo9wbfh89bbdbwfhuezqzogpkmfkjsatibvwk3qxpbvjwcr8i79evui0ab4_a-e7=-6=w200 • javascript:splash_fadeout	com/startapp/sdk/ads/splash/SplashHtml.java
• http://play.google.com • https://play.google.com	com/startapp/sdk/adsbase/a.java
• https://imp.startappservice.com/tracking/adimpression	com/startapp/sdk/adsbase/AdsConstants.java
• https://support.startapp.com/hc/en-us/articles/360002411114	com/startapp/sdk/adsbase/k.java
• https://d1byvlfiet2h9q.cloudfront.net/inapp/resources/adinformationdialog3.html • https://www.com.startapp.com/policy/sdk-policy/ • https://info.startappservice.com/inapp/resources/img1.png	com/startapp/sdk/adsbase/adinformation/AdInformationConfig.java
• javascript:startappbackpressed	com/startapp/sdk/adsbase/consent/ConsentActivity.java
• https://infoevent.startappservice.com/tracking/infoevent	com/startapp/sdk/adsbase/infoevents/AnalyticsConfig.java
• https://adsmetadata.startappservice.com/1.5/ • https://req.startappservice.com/1.5/	com/startapp/sdk/adsbase/remoteconfig/MetaData.java
• https://d2to8y50b3n6dq.cloudfront.net/truststores/ • https://geoip.api.p3insight.de/geoip/	com/startapp/sdk/insight/NetworkTestsMetaData.java

• https://lh6.ggpht.com/vo9wbfh89bbdbwfhuezqzogpkmfkjsatibvwk3qxpbvjwcr8i79evui0ab41a-je7x-6=w200 • javascript:splash_fadeout • https://support.startapp.com/hc/en-us/articles/360002411114 • https://d2to8y50b3n6dq.cloudfront.net/truststores/ • https://geoip.api.c0nnectthed0ts.com/geoip/ • https://play.google.com • https://geoip.api.p3insight.de/geoip/ • https://ul.api.c0nnectthed0ts.com/ul/v3/ • https://d1byvlfiet2h9q.cloudfront.net/inapp/resources/adinformationdialog3.html • https://awsdus.api.p3insight.de/isupload/upload_check_lumen.php • https://daneden.me/animate • https://www.com.startapp.com/policy/sdk-policy/ • 127.0.0.1 • 10.0.2.15 • javascript:startappbackpressed • http://play.google.com • https://mavecy.site/ • https://info.startappservice.com/inapp/resources/info_l.png	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

第三方追踪器检测

名称	类别	网址
IAB Open Measurement	Identification, Advertisement	https://reports.exodus-privacy.eu.org/trackers/328
Startapp	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/195

敏感凭证泄露检测

可能的密钥
com/Vo9wbFH89BbDbWFhUezQZOGPKmfkJSAtIbVWk3QxPbvJwcR8I79EVuI0aB41a
3A757365722F72656C656173652D6B657973
2F73797374656D2F6C69622F6C69627265666572656E63652D72696C2E736F

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隐患。