



ANDROID 静态分析报告



AndaliCash v1.0.0.0.1

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-07-07 07:47:09

i应用概览

文件名称:	AndaliCash v1.0.0.0.1.apk
文件大小:	3.63MB
应用名称:	AndaliCash
软件包名:	icedfcec.dgdeidbd.ddcacdae.dafbfief
主活动:	icedfcec.dgdeidbd.ddcacdae.dafbfief.LaunchActivity
版本号:	1.0.0.0.1
最小SDK:	21
目标SDK:	32
加固信息:	自定义加固
开发框架:	Java/Kotlin
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	1/432
杀软检测:	8 个杀毒软件报毒
MD5:	5ea4976b98ea39de42a95b2fbc707fcd
SHA1:	421f468106a3fa9e7c3852694dbe9b1f32f07429
SHA256:	f475a31063a10b69834b8dd04844408913def4189135b4739a8d8ed27b914dbb

分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✓ 安全	🔍 关注
3	11	2	2	1

四大组件导出状态统计

Activity组件: 5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

APK已签名
 v1 签名: True
 v2 签名: True
 v3 签名: True
 v4 签名: False
 主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
 签名算法: rsassa_pkcs1v15
 有效期自: 2008-02-29 01:33:46+00:00
 有效期至: 2035-07-17 01:33:46+00:00
 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
 序列号: 0x936eacbe07f201df
 哈希算法: sha1
 证书MD5: e89b158e4bcf988ebd09eb83f5378e87
 证书SHA1: 61ed377e85d386a8dfce6b864bd85b0bfaa5af81
 证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
 证书SHA512:
 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640103581053abfea303977272117959704d89b7711292a4569

公钥算法: rsa
 密钥长度: 2048
 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e35
 共检测到 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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.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。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。

android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
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_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
android.permission.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ_PHONE_STATE授予的功能的一个子集，但对即时应用程序不公开。
android.permission.WRITE_CALENDAR	危险	添加或修改日历活动以及向邀请对象发送电子邮件	允许应用程序添加或更改日历中的活动，这可能会向邀请对象发送电子邮件。恶意应用程序可能会借此清除或修改您的日历活动，或者向邀请对象发送电子邮件。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android 8.0 以上系统允许安装未知来源应用程序权限。
android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或SIM卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.PACKAGE_USAGE_STATS	签名	更新组件使用情况	允许修改组件使用情况统计
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
com.google.android.finsky.permission.SIGNATURE_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。

🔒 网络通信安全风险分析

高危: 0 | 警告: 0 | 信息: 0 | 安全: 1

序号	范围	严重级别	描述
1		安全	基本配置配置为禁止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	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@xml/daiaibac]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	Activity (icedfcec.dgdeibd.ddcacdae.dafbfief.Main Activity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

代码安全漏洞检测

高危: 3 | 警告: 7 | 信息: 2 | 安全: 1 | 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: MST G-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入临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MST G-STORAGE-2	升级会员: 解锁高级权限
3	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: MST G-NETWORK-4	升级会员: 解锁高级权限

4	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
5	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
6	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
7	已启用远程WebView调试	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
8	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-14	升级会员: 解锁高级权限
9	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
10	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员: 解锁高级权限

11	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员: 解锁高级权限
12	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
13	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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员: 解锁高级权限
00033	查询IMEI号	信息收集	升级会员: 解锁高级权限
00067	查询IMSI号码	信息收集	升级会员: 解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员: 解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员: 解锁高级权限
00063	隐式意图 (查看网页、拨打电话等)	控制	升级会员: 解锁高级权限
00051	通过Intent隐式意图 (查看网页、拨打电话等)	控制	升级会员: 解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员: 解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员: 解锁高级权限
00189	获取短信内容	短信	升级会员: 解锁高级权限
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员: 解锁高级权限
00054	从文件安装其他APK	反射	升级会员: 解锁高级权限
00202	打电话	控制	升级会员: 解锁高级权限
00203	将电话号码放入意图中	控制	升级会员: 解锁高级权限

00188	获取短信地址	短信	升级会员: 解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员: 解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员: 解锁高级权限
00011	从 URI 查询数据 (SMS、CALLLOGS)	短信 通话记录 信息收集	升级会员: 解锁高级权限
00010	读取敏感数据 (SMS、CALLLOG) 并将其放入 JSON 对象中	短信 通话记录 信息收集	升级会员: 解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员: 解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员: 解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员: 解锁高级权限
00077	读取敏感数据 (短信、通话记录等)	信息收集 短信 通话记录 日历	升级会员: 解锁高级权限
00052	删除内容 URI 指定的媒体 (SMS、CALL_LOG、文件等)	短信	升级会员: 解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员: 解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员: 解锁高级权限
00100	检查网络连通性	信息收集 网络	升级会员: 解锁高级权限
00125	检查指定的文件路径是否存在	文件	升级会员: 解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员: 解锁高级权限
00153	通过 HTTP 发送二进制数据	http	升级会员: 解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员: 解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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	13/30	android.permission.READ_CALL_LOG android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.READ_CALENDAR android.permission.WRITE_CALENDAR android.permission.CALL_PHONE android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_CONTACTS android.permission.GET_ACCOUNTS android.permission.READ_SMS android.permission.PACKAGE_USAGE_STATS
其它常用权限	9/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
pagead2.google syndication.com	安全	是	IP地址: 180.163.150.166 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224333 经度: 121.468948 查看: 高德地图
sattr.s	安全	否	No Geolocation information available.
sadrev...e.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
www.andalicaashop.com	安全	否	IP地址: 47.236.143.4 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
sregister.s	安全	否	No Geolocation information available.

slaunches.s	安全	否	No Geolocation information available.
sconversions.s	安全	否	No Geolocation information available.
sstats.s	安全	否	No Geolocation information available.
sinapps.s	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
<ul style="list-style-type: none"> https://plus.google.com/ 	c/e/a/c/c/l/a.java
<ul style="list-style-type: none"> https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps 	c/e/a/c/a/a/a.java
<ul style="list-style-type: none"> https://%sstats.%s/stats https://%smonitorsdk.%s/remote-debug?app_id= 	c/b/h/k.java
<ul style="list-style-type: none"> https://%sattr.%s/api/v https://%sinapps.%s/api/v https://%sadrevenue.%s/api/v https://%sconversions.%s/api/v https://%slaunches.%s/api/v 	c/b/h/m.java
<ul style="list-style-type: none"> https://www.andalichashbiz.com/memo/v2/app/collect https://www.andalichashbiz.com/#/? https://www.andalichashbiz.com/memo/v2/init https://phl-domain.oss-cn-hongkong.aliyuncs.com/andalichash.txt 	com/cash/lemoloan/statisticlib/StatisticContent.java
<ul style="list-style-type: none"> https://%sregister.%s/api/v 	c/b/h/w.java
<ul style="list-style-type: none"> https://play.google.com/store/apps/details?id= 	icedfcec/dgdeidbd/ddcacdae/dafbfief/MainActivity.java
<ul style="list-style-type: none"> javascript:_javascriptbridge_.javaCallback javascript:_javascriptbridge_.ishandler 	c/c/a/b/g.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52

🔑 敏感凭证泄露检测

可能的密钥
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
13a789c2dd194cfdbb66c8ccf999ad94

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成