南明离火
移动应用检测平台

ANDROID 静态分析报告

imToken • v1.0

分析日期: 2025-07-04 15:43:54

应用概览

文件名称:	imtoken-v2 (1).apk
文件大小:	47.69MB
应用名称:	imToken
软件包名:	in9qe.lmsbk
主活动:	in9qe.lmsbk.MainActivity
版本号:	1.0
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
开发框架:	React Native
应用程序安全分数:	47/100 (中风险)
杀软检测:	AI评估：安全
MD5:	2fc96dbbfca3673bbc51d9954ff4cee8
SHA1:	5bdb1fea48df6409b695c0c7be0cfaca84232feb
SHA256:	e76abc5705902b30b5bebee484f4b4a2c417fbf76a6463c09def1c93b31411ad

分析结果严重性分布

高危	中危	信息	安全	关注
2	8	3	1	0

四大组件导出状态统计

Activity组件：2个，其中export的有： 0个
Service组件：4个，其中export的有： 0个
Receiver组件：2个，其中export的有： 1个
Provider组件：5个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=admind9sxdk, ST=admind9sxdk, L=admind9sxdk, O=admind9sxdk, OU=admind9sxdk, CN=admind9sxdk
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-04 07:15:57+00:00
有效期至: 2125-06-10 07:15:57+00:00
发行人: C=admind9sxdk, ST=admind9sxdk, L=admind9sxdk, O=admind9sxdk, OU=admind9sxdk, CN=admind9sxdk
序列号: 0x62b25dec
哈希算法: sha256
证书MD5: 910f0eb67a1173ae79c72246c892e9b3
证书SHA1: 09fae2d51ea02cf5e175b25282ec612bd78f34fc
证书SHA256: b091ca2db04af9742fe0704c42ba4172d0dab690449d076f680ff8f001f51450
证书SHA512:
83ecb68b5b477ac10df95fb7dddc5f8b79f08fb6dffe288afff96fa20a5189ec89cafa15457779bef02b1607f7308ccd9f193a36b081282e3258d367bc169c89

公钥算法: rsa
密钥长度: 1024
指纹: c669c706b8fd6248a28296f3432ec8ff90d2f8a4003285bd74863fa05d3c4e3a
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.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.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.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
in9qe.lmsbk.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.google.android.finsky.permission.BIND_GET_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

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **0** | 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	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **2** | 警告: **6** | 信息: **3** | 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	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

3	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
4	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
5	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
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
7	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	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-10	升级会员：解锁高级权限
9	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
10	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

11	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)

1	arm64-v8a/libappmodules.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk']	True info 符号被剥离
2	arm64-v8a/libuxpc-modules-core.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk']	True info 符号被剥离

3	arm64-v8a/libfbjni.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离
4	arm64-v8a/libgesturehandler.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

5	arm64-v8a/libhermes.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk', '__vsnprintf_chk', '__strchr_chk', '__write_chk', '__memcpy_chk']	True info 符号被剥离
6	arm64-v8a/libhermestooling.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk']	True info 符号被剥离

7	arm64-v8a/libjsi.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memcpy_chk', '__fwrite_chk', '__strncat_chk', '__write_chk']	True info 符号被剥离
8	arm64-v8a/libreactnative.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk', '__memcpy_chk', '__vsnprintf_chk', '__memset_chk', '__fwrite_chk', '__strncat_chk', '__write_chk']	True info 符号被剥离

9	arm64-v8a/libreactnativequickcrypto.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk', '__memcpy_chk']	True info 符号被剥离
10	arm64-v8a/libreanimated.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk']	True info 符号被剥离

11	arm64-v8a/libworklets.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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
00024	Base64解码后写入文件	反射 文件	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
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setData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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00043	计算WiFi信号强度	信息收集 WiFi	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
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	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	1/30	android.permission.CAMERA
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVIC E

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
twitter.com	安全	否	**IP地址:** 151.101.64.84 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

reactnative.dev	安全	否	**IP地址:** 54.215.62.21 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
pinterest.com	安全	否	**IP地址:** 151.101.64.84 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
filesystem.local	安全	否	No Geolocation information available.
docs.swmansion.com	安全	否	**IP地址:** 172.67.142.188 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://github.com/csstree/csstree/issues • https://co.tatum.io/docsCZEconomicalafriobliberChecksum32_3Non-witness • https://token.im/tos-zh.htmlhandleCreate • https://react.dev/link/refs-must-have-owner • https://www.apifox.cn • http://fb.me/use-check-prop-types • https://docs.ethers.org/api-keys/CommissionAdapterResolutionParseErrorThrowomanchalecologiabsoluteLengthOr0IfBorderTopStyleNoneOrHiddenglobergba • https://support.token.im/hc/articles/24991267493217717e5e1357280ba488085a357904f7d0e1b2d87f0438afcb58ac925ae057 • https://smartbch.graphattendenceheadSymbolOvattivaretaddTracemrzutostateNumericDecimalovattr • https://tzstats.computeExpirationTimechanicannot • http://help.dottoro.com/lcbixvwh.phpalivomissed • https://unhooks.js.org/hooks/dom/iso-external • https://bugzilla.mozilla.org/show_bug.cgi?id=947588firefox • https://tronscan.io • https://rpc.bitlayer.org/llohttps • https://scroll-sepolia.chainstacklabs.compoundSelector • https://www.blockcham.computeMerkleRouteHashes • https://github.com/mdn/data/pull/431 • https://support.token.im/hc/zh-cn/articles/21070054737049-%E5%A6%82%E4%BD%95%E4%BB%8E-CoinCase-%E6%8F%90%E5%B8%81%E8%87%B3-imToken%EF%BC%9Failed • https://rpc.vizing.composeStyles • https://gasstation-testnet.polygon.technology/v2/accounts/_bulkDestroying • https://sepolia.uniscan.xyzilliqa • https://mrousavy.com/react-native-vision-camera/docs/guides/devicescalarMultBaseItemW	

ithSeparatormentaddInputszks_getConfirmedTokenshowErrorCSS
- https://sepolia.metisdevops.linkedinnerHeighttps
- https://polygonscan.com/44
- https://polygon-amoy-bor-rpc.publicnode
- http://www.ummulqura.org.sa/index.aspx
- https://rpc.blast.iovershootRighttps
- https://twitter.com/imTokenOfficial
- https://explorer.mainnet.aurora.devenirrealtitudebrisadauto
- http://www.staff.science.uu.nl
- https://github.com/charpeni/react-native-url-polyfill
- https://www.mintscan.iohttps
- https://react.dev/link/strict-mode-string-ref.current
- https://echo.walletconnect.commitReconciliationEffectsliznicehttps
- https://github.com/csstree/stylelint-validator/issues/29
- https://co.tatum.io/signupciallowFontScalingetSignatureStatuses24HourClockblockchain.block.get
- https://www.btrscan.computeNewHighWaterMarket
- https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting
- https://co.tatum.io/faucetscrollToIndex
- https://discord.com/invite/imTokenfansi-regexEscapeg
- https://endpoints.omniatech.io/v1/arbitrum/sepolia/publickeyPair2/readynamicArray/redelegationsamuraille/reindexAccount/resolve
- https://sepolia.lineascan
- https://signetfaucet.bublina.eu.org/depositsameAsMinWidthAndMinHeighttps
- https://github.com/consenlabsintoniaccessibilityStatesgrunt-saucelabsoluteLength0ForNoneOrTwoValuesLengthAbsoluteKeywordsPercentagestureEnabledvideoHdrawable-sklabsoluteLengthOr0IfBorderBottomStyleNoneOrHiddengine.io-client
- http://help.dottoro.com/lcrthhhv.phpalandajusternumOctavessoCineCambiographfitibiaddCustomSourceTransformerCamera
- http://help.dottoro.com/lclhnthl.phpalacebrunetkaktuseEventTarget
- https://dev.to/li/how-to-requestpermission-for-devicemotion-and-deviceorientation-events-in-ios-13-46g2.8.8ea9666139527a8c1dd94ce4f071fd23c8b350c5a4bb33748c4ba111faccae022c42c2bd4a708b3f5126f16a24ad8b33ba48d0423b6efd5e6348100d8a82Not
- https://github.com/ethers-io/ethers.js/issues/4537
- https://mainnet.aurora.devergonhandleTitleLayoutlook.clamorcerdonitvticolegiovejaugeremoveAnimatedEventFromVieworrybrumeasureLayoutRelativeToContainingList
- https://devnet2openapi.platon.network/rpc.ankr.com/eth_sepoliavanzatoPaget
- https://testnet.blastscan.iohttps
- https://drafts.fxtf.org/css-masking-1
- https://links.ethers.org/v5-errors
- https://co.tatum.io/apps-localstateNode.js
- https://github.com/lahmatiy
- http://help.dottoro.com/lcxquvkf.phpalavradarequestFullscreen-SSL_OP_DONT_INSERT_EMPTY_FRAGMENTSGDPInterestoreFormPadding
- https://docs.expo.dev/workflow/prebuild/.krskavkassertProxies-CLIENT
- http://help.dottoro.com/lcbkewgt.phpaliconmissed
- https://testnet-scan.bitlayer.org
- https://explorer.vizing.comodorizadorflirtucanormal
- https://testnet-zkevm.polygonscan
- https://sepolia-rollup.arbitrum.io/rpcBatchFetchMessages
- https://evm.confluxscan.net/icss
- https://testnet.aurora.devoirrigatoHaveAnimatedStylecheckAtrulePreludevotadovozcexclusivecleanCodevoterproposale
- https://scroll-testnet-public.unifra.iohttps
- https://sepolia.blast.iohttps
- https://zkevm.polygonscan.comumieinvalid
- https://co.tatum.io/faucets-jest-environment-nodejs.stream.disturbednachytatuajedleCannot
- https://github.com/mobxjs/mobx/blob/main/packages/mobx/src/errors.tsaluteInvalid
- https://co.tatum.io/start

目标引擎-A

本报告由南明离火移动安全分析平台生成

• https://testnet.aurorascan.dev/detectAddress • https://token-profile.token.im/asset/bip122/000000000019d6689c085ae165831e93/native/0x0000000000000000000000000000000000000000?symbol=QlRD&locale=zh-CN&utm_source=imtokenAmountExpected • https://www.oklink.com/x1-testigourmandroid.permission.ACTIVITY_RECOGNITIONNativeIdleCallbacksCxxxxxxxx-xxxx-4xxx-yxxx-xxxxxxxxxxxxhdpierreurgba • https://kusama.subscan • https://support.token.im/hc/zh-cn/articles/7221827521305-%E5%A6%82%E4%BD%95%E4%BB%8E%E6%AC%A7%E6%98%93%EF%BC%88OKX%EF%BC%89%E6%8F%90%E5%B8%81%E8%87%B3-imToken%EF%BC%9Failed • https://explorer.zklink • http://phrogz.net/tmp/canvas_image_zoom.htmlhovinanoidinvert • https://socket.io/docs/v3/migrating-from-2-x-to-3-0 • https://rpc.xlayer.technikaddAddressNoteListfunction • https://zksync2-mainnet.zksync.iohubenostaggerhublotrlostaticValuehue • https://docs.swmansion.com/react-native-reanimated/docs/fundamentals/glossary • https://rpc.hekla.taiko • https://react.dev/link/invalid-hook-call • https://evm-t3.cronos.org.ethers.plugins.network.GasCostPluginject • https://rpc.mintchain.iohttps	
• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookShare.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramStoriesShare.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
• https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting#mismatch-between-java-code-version-and-c-code-version • https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting#java-side-failed-to-resolve-c-code-version	com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java
• https://play.google.com/store/apps/details?id=com.discord	cl/json/social/DiscordShare.java
• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookPagesManagerShare.java
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramShare.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenModalFragment.java
• https://twitter.com/intent/tweet?text={message}&url={url}	cl/json/social/TwitterShare.java
• http://filesystem.local	expo/modules/fetch/OkHttpFileUrlInterceptor.java
• https://github.com/software-mansion/react-native-screens/issues	com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java
• http://filesystem.local	expo/modules/fetch/OkHttpFileUrlInterceptorKt.java

• https://github.com/software-mansion/react-native-screens/issues	com/swmansion/rnscreens/InsetsObserverProxy.java
• https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rngh enabledroot	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java
• 192.0.0.3 • 192.0.0.6 • 192.0.0.2 • 192.0.0.1 • 192.0.0.5 • 192.0.0.7 • 192.0.0.4	com/pusherman/networkinfo/RNNetworkInfo.java
• https://pinterest.com/pin/create/button/?url={url}&media=$media&description={message}	cl/json/social/PinterestShare.java
• file:line	lib/arm64-v8a/libjsi.so
• https://reactnative.dev/docs/debugging • file:line	lib/arm64-v8a/libreactnative.so
• data::getsymmetrickeysize • data::getasymmetrickey • data::getsymmetrickey	lib/arm64-v8a/libreactnativequickcrypto.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Jetpack Graphics	Google	利用多个 Android 平台版本中的图形工具降低画面延迟。
BarHopper	Google	BarHopper 是一个 ML Kit 中的库，用于在 Android 设备上识别或解码条形码。
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
C++ 共享库	Android	在 Android 应用中运行原生代码。
OpenSSL	OpenSSL	OpenSSL 是用于传输层安全性协议（TLS）和安全套接字层（SSL）协议的功能强大的，商业级且功能齐全的工具包。
React Native	Facebook	React Native 使你只使用 JavaScript 也能编写原生移动应用。 它在设计原理上和 React 一致，通过声明式的组件机制来搭建丰富多彩的用户界面。
Facebook SDK	Facebook	Facebook SDK是适用于 Android 的将 Facebook集成到 Android 应用程序中的最简单方法。
Hermes JS Engine	Facebook	Hermes 是一个为 React Native 应用程序的快速启动而优化的 JavaScript 引擎。它具有提前静态优化和紧凑的字节码。
Jetpack Camera	Google	CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地向应用添加相机功能。该库提供了很多兼容性修复程序和解决方法，有助于在众多设备上打造一致的开发者体验。
React Native Reanimated	software-mansion	Reanimated is a React Native library that allows for creating smooth animations and interactions that run on the UI thread.

本报告由南明离火移动安全分析平台生成

React Native Screens	software-mansion	React Native Screens is the core library that provides native navigation components to most React Native apps.
React Native Vision Camera	mrousavy	VisionCamera is a powerful Camera library React Native featuring Photo and Video capture, as well as Frame Processing and QR Code scanning.
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。
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

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。