



ANDROID 静态分析报告



Facebook破解 1.0

分析日期: 2025-11-21 17:34:22

i应用概览

文件名称:	Facebook破解.apk
文件大小:	14.02MB
应用名称:	Facebook破解
软件包名:	com.abc4efd1c
主活动:	com.abc4efd1c.MainActivity
版本号:	1.0
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	React Native
应用程序安全分数:	53/100 (中风险)
杀软检测:	AI评估: 安全
MD5:	31b0ea0f8298efd38f8c36296140e1bc
SHA1:	53d90d518a3a85026c3bf84fb741f0e491b60d59
SHA256:	26a3c9b43a0863279a484571785e2e93fbc765c079a17b229586777666ae440

📊分析结果严重性分布

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
2	9	1	2	0

📦四大组件导出状态统计

Activity组件: 1个, 其中export的有: 0个
Service组件: 0个, 其中export的有: 0个
Receiver组件: 1个, 其中export的有: 1个
Provider组件: 2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=YourCountry, ST=YourState, L=YourCity, O=YourOrg, OU=YourOrgUnit, CN=YourName
签名算法: rsassa_pkcs1v15
有效期自: 2025-11-06 05:52:04+00:00
有效期至: 2053-03-24 05:52:04+00:00
发行人: C=YourCountry, ST=YourState, L=YourCity, O=YourOrg, OU=YourOrgUnit, CN=YourName
序列号: 0x9c19f96802907cf3
哈希算法: sha256
证书MD5: 8e6cba3c32fd2b57d3563738fdec4526
证书SHA1: c58c743633a107bc3ff1dad05f2cbd9351fecee5
证书SHA256: 7011c7bc98a69ba8bd568023b56d017fce74c59fb85a55fcab0433df1f57c259
证书SHA512:
bcce13b11ed3d63296032170aae5d52dac665dd72ae2763a027d9ed076bacf5e85cb57d2560c4327eb837ce9e3ccdc3219061d17d4ce37d405dcfa8c2cb2623

公钥算法: rsa
密钥长度: 2048
指纹: a0bb43c4341a8372747b22029b1b53f28d82c72f874f4eb658595ab58405bdc0
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.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。
com.abc4efd1c.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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	严重程度	描述
----	----	------	----

证书安全分析

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: 1 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	Broadcast Receiver (android.x.profileinstaller.ProfileInstallerReceiver) 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: 7 | 信息: 1 | 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: MSTG-STORAGE-3	升级会员: 解锁高级权限
2	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
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	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
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	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
7	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: MSTG-STORAGE-2	升级会员: 解锁高级权限
8	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

9	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
10	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
11	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

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/libfb.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH。	No n e 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。	Tr u e in fo 符号被剥离
2	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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH。	No n e 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。	Tr u e in fo 符号被剥离

3	arm64-v8a/libglog.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH。	No n e 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: ['__memcpy_chk', '__strlen_chk', '__strncat_chk', '__vsnprintf_chk']	Tr u e info 符号被剥离
4	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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH。	No n e 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: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__strchr_chk']	Tr u e info 符号被剥离

5	arm64-v8a/libhermes_executor.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH。	No n e 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', '__memset_chk', '__vsprintf_chk', '__read_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk']	Tr u e info 符号被剥离
6	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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH。	No n e 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']	Tr u e info 符号被剥离

7	arm64-v8a/libreactperfloggerjni.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	No n e 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。	Tr u e info 符号被剥离
8	arm64-v8a/librcc_image.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	No n e 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。	Tr u e info 符号被剥离

9	arm64-v8a/librrc_legacyviewmanagerinterop.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	No n e 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。	Tr u e info 符号被剥离
10	arm64-v8a/librrc_root.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。	No n e info 二进制文件没有设置运行时搜索路径或RPATH	No n e 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。	Tr u e info 符号被剥离

11	arm64-v8a/librrc_scrollview.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH。	No n e 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
12	arm64-v8a/librrc_text.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH。	No n e 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

13	arm64-v8a/librrc_textinput.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	No n e 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。	Tr u e info 符号被剥离
14	arm64-v8a/librrc_unimplementedview.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	No n e 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。	Tr u e info 符号被剥离

15	arm64-v8a/librrc_view.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。	No ne inf o 二进制文件没有设置运行时搜索路径或 RPATH	N o n e i n f o 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['_vsprintf_chk']	Tr u e i n f o 符号被剥离
----	--------------------------	---	--	---	--	---	---	---	--

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
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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00162	创建 InetAddress 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
00056	修改语音音量	控制	升级会员：解锁高级权限
00028	从assets目录中读取文件	文件	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
00114	创建到代理地址的安全套接字连接	网络 命令	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
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	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

00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	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
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
00132	查询ISO国家代码	电话服务 信息收集	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
00188	获取短信地址	短信	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
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

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	2/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE

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
aomedia.org	安全	否	IP地址: 185.199.108.153 国家: 美国 地区: 宾夕法尼亚 城市: 加利福尼亚 纬度: 40.065647 经度: -79.891724 查看: Google 地图

dashif.org	安全	否	IP地址: 185.199.110.153 国家: 美国 地区: 宾夕法尼亚 城市: 加利福尼亚 纬度: 40.065647 经度: -79.891724 查看: Google 地图
www.android.com	安全	否	IP地址: 142.251.39.142 国家: 美国 地区: 加利福尼亚 城市: 山景城 纬度: 37.386051 经度: -122.083817 查看: Google 地图
default.url	安全	否	No Geolocation information available.

🌐 URL 链接安全分析

URL信息	源码文件
- http://fb.me/use-check-prop-typest-control-rodentCan - https://bit.ly/3cXEKwfinishClassComponentable-key-changeIndexpires=Unknown - https://redux.js.org/Errors?code=&hash=2&size==TONALPHABEThe	自研引擎A
http://%s/status	l7/k.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/o.java
- data:cs:audiopurposecs:2007 - file:dvb-dash: - http://dashif.org/guidelines/thumbnail_tile - http://dashif.org/thumbnail_tile - http://dashif.org/guidelines/last-segment-number - http://dashif.org/guidelines/trickmode	a1/d.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/s.java
10.0.1.1	i7/b.java
- https://developer.apple.com/streaming/emsg-id3 - https://aomedia.org/emsg/id3	d2/a.java
10.0.2.2 10.0.3.2	v7/a.java
https://default.url	b1/n0.java

- file:dvb-dash: 10.0.1.1 - data:cs:audiopurposesecs:2007 - https://default.url - https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067 - http://dashif.org/guidelines/thumbnail_tile 10.0.3.2 - http://www.android.com/ - http://dashif.org/guidelines/trickmode - http://%/s/inspector/device?name=%s&app=%s - ws://%/s/debugger-proxy?role=client - http://%/s/launch-js-devtools - https://developer.apple.com/streaming/emsg-id3 - https://aomedia.org/emsg/id3 - http://%/s/status - http://dashif.org/thumbnail_tile - http://dashif.org/guidelines/last-segment-number 10.0.2.2 - http://%/s/open-url - http://%/s/%s.%s?platform=android&dev=%s&minify=%s&app=%s&modulesonly=%s&runmodule=%s %s	自研引擎-S
file:line	lib/arm64-v8a/libglog.so
18.244.0.188 1.2.3.4	lib/arm64-v8a/libhermes_executor.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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构建丰富多彩的用户界面。
Facebook SDK	Facebook	Facebook SDK 是用于 Android 的将 Facebook 集成到 Android 应用程序中的最简单方法。
Folly	Facebook	An open-source C++ library developed and used at Facebook.
GIFLIB	GIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs since 1989. It is deployed everywhere you can think of and some places you probably can't - graphics applications and web browsers on multiple operating systems, game consoles, smartphones, and likely your ATM too.
glog	Google	glog 是一个 C++ 日志库，它提供 C++ 流式风格的 API。
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。
Yoga	Facebook	Yoga 意在打造一个跨 iOS、Android、Windows 平台在内的布局引擎，兼容 Flexbox 布局方式，让界面布局更加简单。
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.

Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。

🔑 敏感凭证泄露检测

可能的密钥
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

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