



■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: Al评估: 安全

MD5: 31b0ea0f8298efd38f8c36296140e1bc

SHA1: 53d90d518a3a85026c3bf84fb74-c1e491360d59

SHA256: 26a3c9b43a0863279a48457 1785 22e93fbcb765c07(a17,3229) 86777666ae440

₿分析结果严重性分布

★高危	▲ 中心	iash	✔ 安全	《 关注
2		1	2	0

■四大组件异出状态统计

Activity组、一个,其中export的对人。
Service组件: 0个,其中export的有,0个
Receiver组件: 1个,14)export的有: 1个
Provider组件、2个 其中export的有: 0个

常应用签名证书信息

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:

bcce13b11ed3d63296032170aae5d52dac665dd72ae2763a027d9ed076bacf5e85cb57d2560c4327eb837ce9e3ccdc3219061d131d4ce37d405dcfa8c2cb2623

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	人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_EXPORTE D_PERMISSION	未知	未知友限	来自 and rold 引用的未知权限。

■ 网络通信安全风险分析

序号	范围	平重赤别	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 位別已使用代码签名证书进行签名。

Q Mannest 配置安全分析

高危: 0 | 警告: 1 | 信息: 0 | 昇藤: 0

序号	问题	严重程度	描述信息
1	Broadcast Receiver (android x.profile installer.Profile Install Receiver) 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: In sufficient Cryptograph y OWASP MASVS: MSTG- CRYPTO-6	升级会员:解《葡夏校限
4	IP地址泄露	警告	CWE: CWE-200: 信息機 露 OWASP MASVS: MS LG CODE-2	升级会员:解锁高级权器
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 KWI-276: 默认权 限入证确 OWASN Top 10: M2: In occure Data Storage OWASP MASVS: MSVG- STORAGE-2	天你会员:解锁高级权限
6	此应用程序使用SSL Pinning 来於學 或防止安全通信通道中的MITM改畫	安全	OWASP MATVS: MSTG- NPTLY ARX-4	升级会员;解锁高级权限
7	应用程序创建增时文件。敏感信息永远不应该被与五届计文件		CWE: CWE-276: 默认权 PRATE确 OWASP Top 10: M2: In secure 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对Wer-View.loadDataWithBaseUNJ分,采加载一个网页到Web eyr,那么这个应用程序可能会遭受够处地。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: Im proper Platform Usag e OWASP MASVS: MSTG- PLATFORM-6	升级会员:解锁高级权限

南明离火多	安全分析平台	技术分析报告	MD5: 31b	<u>0ea0f8298efd38f8c</u>	36296140e1bc			
9	文件可能包含硬绘用户名、密码、图	扁码的敏感信息,如 密钥等	警告	CWE: CWE-312: 明文存 储敏感信息 OWASP Top 10: M9: Re verse Engineering OWASP MASVS: MSTG- STORAGE-14	升级会员:解锁高;	级权限		
10	SHA-1是已知存在	E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: In sufficient Cryptograph y OWASP MASVS: MSTG- CRYPTO-4	升级会员:解锁高红	级权限	X A	
11		PKCS5/PKCS7填充的 比配置容易受到填充o	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: In sufficient Cryptograph y OWASP MASVS: MSTG- CRYPTO-3	升级会员:解键高	愛校限		
► Nat	tive 库安全	全加固检测		<i>i</i>	17/	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	\(\)	
序号	if the second of	NX(抽動 禁心執 行	PIE	STACK GANIAR 火起菜户)	RELRO	RUNPATH(指定SO搜索路径)	FORTIFY(常用函数加强检查)	SYMBOLSSTRPPED(裁剪符号表)
>	C XIA-Y							

南明	离火安全分析平台 技术	分析报告	MD5: 31b0	ea0f8298efd38f	8c36296140e1bc				
1	arm64-v8a/libfb.so	True info 二件设位。文字 NX标存可使者的 C 表面行攻入 市场 T 表面行攻入 市场 T 表面行攻入 市场 T 表面行攻入 T 表面 T 表	动象(DSO) info 共享的使用,是不够的,是是不够的,是是不够的,是是不够的,是是不够的,是是不够的,是不够的,	True info 这个二进制文件在栈上添加了一个样上添值,以便它会被溢出返回地上流。在这种正义,这是这种的一个,这是这种,这是这种,这是这种,这是这种,这是这种,这是这种,是这种,是这种,是	Full RELRO info 此共享对象已完全 启用 RELRO。REL RO 确保 GOT 不会 在易受攻击的 ELF 二进制 产生 RELRO 中,整个 GOT (.go t 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和企或PATH	Noneinfo二进制文件没有设置RUNATH	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_S OURCE=2 来加固函数。这个检查对于 Dart/Flutt er 库不适用	Tr u e in fo符号被剥离
2	arm64-v8a/libfbjni.so	True info 二件以位表面,在这个人,并不可使者的。 这内不可使者的,在这个人,在这个人,在这个人,在这个人,在这个人,在这个人,在这个人,在这个人	动象(DSO) info 共享的使用,用,fPIC,用,是是标该与的使用。 有是是一个,用一个,是一个,是一个,是一个。 的编程。(NO P),在一个,是一个,是一个,是一个,是一个,是一个,是一个,是一个,是一个,是一个,是	True info 这个二进制文件 在栈上哨兵作。以 便它会被潘迅河。 个栈全被潘迅河。 「阿龙河河河河河河河河河河河河河河河河河河河河河河河河河河河河河河河河河河河河	Full relaco is 10 此共享对象已完全 后用 RELRO。 REL RO 确保 GOT 不会 在易受攻击的 EL 二进制文件中块覆 盖。在完整 RELRO 中,整个 GOT (.go t II sot plt 两者) 被标记生只读。	No ne	Zon quinfo二进制文件没有设置RUNPATH	alse yarning 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_S OURCE=2 来加固函数。这个检查对于 Dart/Flutt er 库不适用	Tr u e in fo 符号被剥离
	W. J. W. W. J. W.								

南明	离火安全分析平台 技术	分析报告	MD5: 31b0	ea0f8298efd38f	8c36296140e1bc				
3	arm64-v8a/libglog.so	True info 二件以后,这内不,由的 文字 NX 标存可使者注明。 着面行攻入的 shellco de 不。	动象(DSO) info 共享PIC 中国的原理的,并不是不是的,是是不是的,是是不是的,是是不是的,是是不是的,是是不是的,是是不是的,是是不是的,是是不是的。	True info 这个二进制文件在栈上添加了个件在栈上添加了一个样点。在核上添加了一个大大。这一个大大的一个大大的。这个一个大大的一个大大的。这个一个大大的一个大小的一个大小的一个大小的一个大小的一个大小的一个大小的一个大小	Full RELRO info 此共享对象已完全 启用 RELRO。REL RO 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(.go t 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和企或及A H	Noneinfo二进制文件没有设置RUNATH	True info 二进制文件有以下加固函数: ['memcpy_chk', ' strlen_chk', 'strncat_c hk', 'vsnprintf_chk']	Tr u e in fo符号被剥离
4	arm64-v8a/libhermes.so	True info 二件设位。 一件以位。 一件以位。 一种以位。 一种,以一种,一种,一种,一种,一种,一种,一种,一种,一种,一种,一种,一种,一种,一	动象(DSO) info 共享的使用人。 中,是是一个,是是一个,是一个,是一个,是一个,是一个,是一个,是一个,是一个,是	True info 这个二进制文件在栈上课年10 人工进制工了一个便宜,在楼上课年10 人工证明,这种可以通过的一个更过的一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	Full Kel RO it 10	No ne ne no ne	Z on e in fo 二进制文件没有设置R U N P A T H	rive j no 一进制文件有以下加固函数: ['memcpy_chk', ' strlen_chk', 'vsnprintf _chk', 'strchr_chk']	Tr u e in fo 符号被剥离
	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX								

刊 円	离火安全分析平台 技术	分析报告	MD5: 31b0e	<u>ea0f8298efd38f</u>	8c36296140e1bc				
5	arm64-v8a/libhermes_exec utor.so	True info 二件以下 info 二件以下 info 二件以下 info 二件以下 info 以下 info info info info info info info info	动态共享对象(DSO) info 共享库足标。 特别是一个,并是一个,并是一个,并是一个,并是一个,并是一个,并是一个,并是一个,并	True info 这个二进制文件在栈上添加值,文件一个栈上添加值,以便它会被从的栈缓冲回地上,这一个大大小人。 这一个时间,这一个大大小人,这一个一个大大小人,这一个一个大小人,就是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	Full RELRO info 此共享对象已完全启用 RELRO。REL RO 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(.go t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品径或 NA H	Noneinfo二进制文件没有设置RUNATH	True info 二进制文件有以下加固函 数: ['strlen_chk', 'me mcpy_chk', 'memset_c hk', 'vsnprintf_chk', ' read_chk', 'FD_CLR_ch k', 'FD_ISSET_chk', 'F D_SET_chk']	Trueinfo符号被剥离
6	arm64-v8a/libjsi.so	True info 二件放射 在 c c c c c c c c c c c c c c c c c c	动象 (DSO) info 共 fPIC ,用关 这 医 (DO) 中 是标 该 与 的 使 医 (DO) 中 不 第 4 第 4 第 4 第 4 第 4 第 4 第 4 第 4 第 4 第	True info 这个人工程,这个工程,这个工程,这个工程,是一个人工程,是一个人们是一个人们,这一个一个人们,这一个一个人们,这一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	Full KelrO in to in the in t	Nonemo二速制文件没有设置运行时搜索路径或RATH	Zon ewin fo 二进制文件没有设置RUNPATH	rue juro 二进制文件有以下加固函 数: ['strlen_chk']	Trueinfo符号被剥离

南明	离火安全分析平台 技术	分析报告	MD5: 31b0	ea0f8298efd38f	8c36296140e1bc				
7	arm64-v8a/libreactperflogg erjni.so	True info 二件以 文字 NX 标志可执得注记 位。 本面行攻 市的 shellco de 不。	动象(DSO) info 共享的是标文的,用一种的工作,并是不是的一种的,用一种的工作。如此,是是一种的一种的一种,是一种的一种。 一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是	True info 这个二进制文件在栈上添加了一个大人,还是一个大人。这个二进制工工,以便它会被溢出这一回地震,这样可以通过的大人。这个一个大人,是一个大人,是一个一个大人,是一个一个大人,是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	Full RELRO info 此共享对象已完全 启用 RELRO。REL RO 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 (.go t 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品企或P A H	None info二进制文件没有设置 R UN A T H	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_S OURCE=2 来加固函数。 这个检查对于 Dart/Flutt er 库不适用	Tr u e in fo 符号被剥离
8	arm64-v8a/librrc_image.so	True info 二件以位,这内不,由于这个不可使者的。有时,这个不可使者的。不可以有对,由于这个不可以有对。	动态(DSO) info 共享的使用,用是一种的。 中,是一种的。 中,是一种的,用一种的。 中,是一种的,是一种的。 中,是一种的。 中,是一种的。 中,是一种的。 中,是一种的。 中,是一种的。	True info 这个二进制文件 在栈上哨兵作。 使它会被流出。 使它会被流出。 使它会处理。这样 反对,是是是一个大型,是是一个大型,是是一个大型,是是一个大型,是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	Full relaco is 10 此共享对象已完全 后用 RELRO。 REL RO 确保 GOT 不会 在易受攻击的 EL 二进制文件中决覆 盖。在完整 VELRO 中,整个 GOT (.go t II gotplt 两者) 被标记生只读。	No ne	Zon winfo二进制文件没有设置RUNPATH	alse yarning 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_S OURCE=2 来加固函数。这个检查对于 Dart/Flutt er 库不适用	Tr u e in fo 符号被剥离
	X A A A A A A A A A A A A A A A A A A A								

南明	离火安全分析平台 技术	分析报告	MD5: 31b0e	ea0f8298efd38f	8c36296140e1bc				
9	arm64-v8a/librrc_legacyvie wmanagerinterop.so	True info 二件以后,这内不,由的 文字 NX 标存可使者注明。 着面行攻入的 shellco de 不。	动象(DSO) info 共享中的原理,是是一个,是是一个,是是一个,是是一个,是是一个,是是一个,是是一个,是一个,	True info 这个二进制文件在栈上添加了个件在栈上添加了一个样点强值,以便它地上透过的。这个正确,这一个大概,是这个一个大概,是这个一个,这个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一	Full RELRO info 此共享对象已完全 启用 RELRO。REL RO 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 (.go t 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品位或及ATH	Noneinfo二进制文件没有设置RUNATH	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_S OURCE=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
10	arm64-v8a/librrc_root.so	True info 二件MX info 二件MX info MX info	动象(DSO) info 共享的使用的原理。 中,用类这级(NO) 中,用类这级(NO) 中,用类这级(NO) 中,用类这级(NO) 中,用类的使用。 中,用类的使用。 中,用类的使用。 中,用类的使用。	True info 这个二进制文件 在栈它上哨会址标。这种可以通常发生,这种可以通常发生,这种可以通常发生。这种可以通常发生,这种可以通常发生。	FLIL CELRO it no	No ne foll 远制文件没有设置运行时搜索路径或 R AT H	Non e in fo 二进制文件没有设置RUNPATH	alse yarning 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_S OURCE=2 来加固函数。 这个检查对于 Dart/Flutt er 库不适用	Tr u e in fo 符号被剥离
	W. W.								

南明	<u> 离火安全分析平台 技术</u>	分析报告	MD5: 31b0e	ea0f8298efd38f	8c36296140e1bc				
11	arm64-v8a/librrc_scrollvie w.so	True info 二件以下 NX 标志可以 A不可使者注明的 文字 NX 标志可以得注明的 文字 NX 标志可以得注明的 Shellco de 不行。	动态(DSO) info 共享存足使用,用是它,用是一种的。 并是一种,用一种,用一种,并不是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,	True info 这个二进制文件在栈上添加了一个栈上添加了一个栈点点,但 使它会被溢出返回地覆盖。这个一个大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大	Full RELRO info 此共享对象已完全 启用 RELRO。REL RO 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(.go t 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品径或 P. A. H	Noneinfo二进制文件没有设置RUNATH	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_S OURCE=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
12	arm64-v8a/librrc_text.so	True info 二件以 Mix 标序可使者 Shell Co de 不, 击的 de 不 fo de	动象(DSO) info 共可的 中,是是一个,是一个,是一个,是一个,是一个,是一个,是一个,是一个,是一个,是一	True info 这个一种,这个一种,这个一种,这个一种,这个一种,这个一种,这个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一	FULL ELRO in	No ne no 一边制文件没有设置运行时搜索路径或RAH	Z O C quin fo 二进制文件没有设置R U N P A T H	alse yarning 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_S OURCE=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
	* A TANK								

南明离火	安全分析平台 技术	分析报告	MD5: 31b0€	ea0f8298efd38f	8c36296140e1bc				
13 arr	m64-v8a/librrc_textinput	True info 二性的 文字 MX 位本表面行为 AX 位本表面行为 不, 击的 Shellco de 不 fo de format de	动象(DSO) info 共 -fPIC 标。 构定是标。 构定是标。 有是一种,用类。 的是一种,用类。 的是一种,用类。 的是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,	True info 这个二进制文件在栈上调单文件在栈上哨兵值,但它是上调点。这个二进制文子一个线点被线线对于区域的线线对于区域的大量,是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	Full RELRO info 此共享对象已完全 启用 RELRO。REL RO 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(.go t 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和企或及AT H	Noneinfo二进制文件没有设置RUNATH	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_S OURCE=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
14	m64-v8a/librrc_unimple entedview.so	True info 二世報 置 c c c c c c c c c c c c c c c c c c	动象(DSO) info 共-fPIC,用关这返 使用关这返 使用关这返 位 中的启无。向程 分 中,用关这返 (DE) 中,用关这。 (DE)	True info 这个工进制文件在栈上端头上端头上端头上。这个工工,这种一个大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大大	Full KelrO ix io 此共享对象已完全 后用 RELRO。REL RO 确保 GOT 不会 在易受攻击的 EL 二进制文件中读覆 盖。在完整《ELRO 中,整个 GOT(.go t、IT、otyplt 两者) 被标为少分读。	No ne	Zon a in fo 二进制文件没有设置RUNPATH	alse yarning 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_S OURCE=2 来加固函数。这个检查对于 Dart/Flutt er 库不适用	Trueinfo符号被剥离

15 arm64-v8a/lil	True info 二进制置了 NX 位。 这标志着 内存可执得注入 的 shellco de 不可执 行。	动象(DSO) info 共用。fPIC,用子这多位,用子这多位,用类这多位,用类的一种的,用类的,用类的,用类的,用类的,用类的,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种	True info 这个二进制文件在栈哨人工进制加工工作。这个二进制加工工作,从便它地看到这个一个人。这个时间,这个时间,这个时间,这个时间,这个时间,这个时间,这个时间,这个时间,	Full RELRO info 此共享对象已完全 启用 RELRO。REL RO 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(.go t 和 .got.plt 两者)被标记为只读。	No ne in o 二进制文件没有设置运行时搜索和企或 P AT H	Noneinfo二进制文件没有设置RUNATH	True info 二进制文件有以下加固函数: ['vsnprintf_chk']	Tr u e in fo 符号被剥离
------------------	--	---	---	---	-------------------------------------	-------------------------	---	--------------------

▲ 应用行为分析

		XXIII	
编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	一级会员: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 InetSocketAddress 对象并发接到2	socket	升级会员:解锁高级权限
00163	创建新的 Socket 并连接到它	ocket	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目录中读文文件	文件	升级会员:解锁高级权限
00077	读 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	创建到代理地址的多全。接字连接	网络命令	升级会员:解锁高级权限
00096	连接對化於人,改置请求方法	命令网络	升级会员:解锁高级权限
00089	主接到 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:解锁高级早里
00189	获取短信内容	短信	升级会员: 44 高级权根
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	一十级会员: 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:解锁高度权限

號::敏感权限滥用分析

类型	匹配	权限 人工
恶意软件常用权限	0/30	
其它常用权限	2/46	android.permission.Acc.135_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

② 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	P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: -122.083847 查看: Google ft 医
default.url	安全	否	No Geol pration information available.

♥ URL 链接安全分析

	X ₃ \\
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/4
• http://%s/status	17/k.java
• https://github.com/software-mansion/react-native-screens/issues//7#issuect-mment-42470406	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/reac_vat/ve-screens/issuet/17#iss/vecomment-42470406	com/swmansion/rnscreens/s.java
• 10.0.1.1	i7/b.java
https://developer.apple.com/streaming/emsg-id3	d2/a.java
• 10.0.2.2 • 10.0.3.2	v7/a.java
https://depaylt.url	b1/n0.java

• file:dvb-dash: • 10.0.1.1 • data:cs:audiopurposecs: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 自研引擎-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 • http://%s/open-url • http://%s/%s.%s?platform=android&dev=%s&minify=%s&app=%s&modulesonly=%s&runmodule=%s • file:line lib/arm64-v8a/lbg • 18.244.0.188 lib/arm 4-y 82 (libkermes_executor.so

\$ 第三方 SDK 组件分析

• 1.2.3.4

SDK名称	开发者	描述信息人
Fresco	<u>Facebook</u>	Fresco 是一个用于管理图像及其使用 in ; 存的 / Indroid 库。
C++ 共享库	<u>Android</u>	在 Android 应用中运行原生代码。
React Native	Facebook	R act Native 使你只使呀 JavaSc ipt 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找建丰富多彩的用户界面。
Facebook SDK	Facebook	Facebook X 以是 有于 Android 的将 Facebook集成到 Android 应用程序中的最简单方法。
Folly	T <u>ice ook</u>	An optin-source C++ library developed and used at Facebook.
GIFLIB	ĞIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs on E-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, smartphon es, 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	<u>Farebrok</u>	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	<u>Facebook</u>	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 interaction s 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。
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	XY-
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 在律法 已能够**有**所以 损失概不负责。本报告内容仅供网络安全研究,不得违反中

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

© 2025 南明离火 - 移动安全分析平台自动生成