



ANDROID 静态分析报告



◆ 彩库宝典 · v2.5.3

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: 2025-03-11 17:28:14

i应用概览

文件名称:	app-200.apk
文件大小:	46.71MB
应用名称:	彩库宝典
软件包名:	com.pjznx.fcqfk
主活动:	com.bjcalculator.tb.launch.StartActivity
版本号:	2.5.3
最小SDK:	24
目标SDK:	31
加固信息:	未加壳
开发框架:	React Native
应用程序安全分数:	51/100 (中风险)
杀软检测:	AI评估: 可能有安全隐患
MD5:	d0081d5126500fbcc1f17f4ef26e3148
SHA1:	39a8aa63bb21f75e3743051d6ac91cd1933898843
SHA256:	65de600d0b9315dc13d8e40a1e97f6f22e2b13b3117177ecee5c5fb9aee4fed50

分析结果严重性

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
1	3	0	1	0

四大组件信息

Activity组件: 24个, 其中export的有: 7个
Service组件: 6个, 其中export的有: 1个
Receiver组件: 0个, 其中export的有: 0个
Provider组件: 0个, 其中export的有: 0个

证书信息

二进制文件已签名

v1 签名: False
 v2 签名: True
 v3 签名: True
 v4 签名: False
 主题: C=Country, ST=State, L=City, O=Company, OU=Dev, CN=Example
 签名算法: rsassa_pkcs1v15
 有效期自: 2025-03-11 09:15:48+00:00
 有效期至: 2052-07-27 09:15:48+00:00
 发行人: C=Country, ST=State, L=City, O=Company, OU=Dev, CN=Example
 序列号: 0xf98a29480a81b3ae
 哈希算法: sha384
 证书MD5: ed1ea7d1c08dc02411799a8021a80a38
 证书SHA1: a1fc2003fef67f86f8d15d8e4c4f37ef2cb42908
 证书SHA256: 4a8308a21f3d0f8319ffc4e958af9cb84a07a6d30ef5db54957538f3bb1404bf
 证书SHA512:
 0e1bafd07cc67f8ffbb43a26057bbefaca0417a61a38c9f3dcd0c1718c68d757b122e93fac52ea521159a4e9facdbfc0fd9af723c94a7ce66bbcf4de34d6c9a

公钥算法: rsa
 密钥长度: 2048
 指纹: aa787ecb85dc41e451941abf2340c53ee3ed55025fc0496532470949d98df3bd
 找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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.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_INTERNAL_STORAGE	未知	未知权限	来自 android 引用的未知权限。
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.BODY_SENSORS	危险	授予对身体传感器的访问权限, 例如心率	允许应用程序访问来自传感器的数据, 用户使用这些传感器来测量身体内部发生的事情, 例如心率。
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。
com.pjznx.fcqfk.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知, Android 13 引入的新权限。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标, 接入vivo平台后需要用户手动开启, 开启完成后收到新消息时, 在已安装的应用桌面图标右上角显示“数字角标”。
com.hihonor.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。

android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器, 用于消息通知振动功能。
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.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限, 则还必须请求ACCESS_COARSE_LOCATION或ACCESS_FINE_LOCATION。单独请求此权限不会授予您位置访问权限。
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.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。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
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。

可浏览的Activity组件

ACTIVITY	INTENT
com.tencent.tauth.AuthActivity	Scheme: tencent101998298://,

网络通信安全

高危: 1 | 警告: 1 | 信息: 0 | 安全: 0

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。
2	*	警告	基本配置配置为信任系统证书。

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: 0 | 警告: 11 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	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。
2	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_config]	信息	网络安全配置功能让应用程序可以在一个安全的, 声明式的配置文件中自定义他们的网络安全设置, 而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
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	Activity (com.bjcalculator.tb.wxapi.WXEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享, 因此可被设备上的任何其他应用程序访问。
5	Activity (com.tencent.tauth.AuthActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享, 因此可被设备上的任何其他应用程序访问。
6	Activity (cn.jpsh.android.ui.PopWinActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享, 因此可被设备上的任何其他应用程序访问。
7	Activity (cn.jpsh.android.ui.PushActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享, 因此可被设备上的任何其他应用程序访问。
8	Activity (cn.jpsh.android.service.JNotifyActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享, 因此可被设备上的任何其他应用程序访问。
9	Activity (cn.android.service.JTransitActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享, 因此可被设备上的任何其他应用程序访问。
10	Activity (cn.jpsh.android.service.DActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享, 因此可被设备上的任何其他应用程序访问。
11	Service (cn.jiguang.plugins.service.JCoreModuleService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享, 因此可被设备上的任何其他应用程序访问。
12	高优先级的Intent (1000) - {1个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级, 应用程序有效地覆盖了其他请求。

</> 安全漏洞检测

序号	问题	等级	参考标准	文件位置
----	----	----	------	------

动态库分析

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/libbetter.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。	False high 这个二进制文件没有在线添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all启用栈哨兵。这对于Dart/Flutter不适用，除非使用了Dart FFI	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

2	arm64-v8a/libfb.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info
3	arm64-v8a/libfbjni.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>True info</p> <p>二进制文件有以下加固函数: ['_strlen_chk']</p>	True info

4	arm64-v8a/libglog.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info
5	arm64-v8a/libhermes.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>True info</p> <p>二进制文件有以下加固函数: ['_strchr_chk', '_strlen_chk', '_vsnprintf_chk', '_memcpy_chk']</p>	True info

6	arm64-v8a/libreactnative_mmkv.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None info	None info	<p>True info</p> <p>二进制文件有以下加固函数: ['_memcpy_chk', '_strlen_chk', '_strcat_chk', '_strchr_chk', '_vsnprintf_chk', '_read_chk']</p>	True info
7	arm64-v8a/libreactperloggerni.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None info	None info	<p>False warning</p> <p>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</p>	True info

8	arm64-v8a/libreanimated.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None info	None info	<p>True info</p> <p>二进制文件有以下加固函数: ['__strlen_chk']</p>	True info
9	arm64-v8a/librcc_image.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None info	None info	<p>False warning</p> <p>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</p>	True info

10	arm64-v8a/librcc_modal.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info
11	arm64-v8a/librcc_picker.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info

<p>1 2</p>	<p>arm64-v8a/librcc_progressbar.so</p>	<p>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。</p>	<p>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。</p>	<p>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</p>	<p>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。</p>	<p>N o n e info 二 进 制 文 件 没 有 设 置 运 行 时 搜 索 路 径 或 R P A T H</p>	<p>N o n e info 二 进 制 文 件 没 有 设 置 R U N P A T H</p>	<p>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</p>	<p>Tr u e in fo 符 号 被 剥 离</p>
<p>1 3</p>	<p>arm64-v8a/librcc_root.so</p>	<p>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。</p>	<p>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。</p>	<p>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</p>	<p>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。</p>	<p>N o n e in fo 二 进 制 文 件 没 有 设 置 运 行 时 搜 索 路 径 或 R P A T H</p>	<p>N o n e in fo 二 进 制 文 件 没 有 设 置 R U N P A T H</p>	<p>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</p>	<p>Tr u e in fo 符 号 被 剥 离</p>

14	arm64-v8a/librcc_scrollview.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info
15	arm64-v8a/librcc_slider.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info

16	arm64-v8a/librcc_switch.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info
17	arm64-v8a/librcc_text.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info

18	arm64-v8a/librcc_textinput.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info
19	arm64-v8a/librcc_unimplementedview.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info

20	arm64-v8a/librcc_view.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info
21	arm64-v8a/libstatic-webp.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>True info</p> <p>二进制文件有以下加固函数: ['_vsprintf_chk', '_strlen_chk', '_memcpy_chk', '_memmove_chk', '_vsprintf_chk']</p>	True info

2 2	arm64-v8a/libyuv_to_rgb_jni.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。	N o n e info 二 进 制 文 件 没 有 设 置 运 行 时 搜 索 路 径 或 R P A T H	N o n e info 二 进 制 文 件 没 有 设 置 R U N P A T H	True info 二进制文件有以下加固函数: ['__memcpy_chk']	Tr u e info 符 号 被 剥 离
--------	--------------------------------	---	---	--	--	---	---	---	--

🍷 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
00013	读取文件并将其放入流中	文件	升级会员: 解锁高级权限

🔍 敏感权限分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.CAMERA android.permission.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.READ_PHONE_STATE android.permission.GET_TASKS
其它常用权限	8/46	android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_BACKGROUND_LOCATION com.google.android.c2dm.permission.RECEIVE 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。

🔍 域名检测

域名	状态	中国境内	位置信息
journeyapps.com	安全	否	IP地址: 13.249.59.9 国家: 美国 地区: 得克萨斯州 城市: 休斯敦 纬度: 29.763029 经度: -95.362067 查看: Google 地图

🌐 URL链接分析

URL信息	源码文件
<ul style="list-style-type: none"> https://journeyapps.com/ https://github.com/journeyapps/zxing-android-embedded 	自研引擎-S
<ul style="list-style-type: none"> file:line 	lib/arm64-v8a/libglog.so

📦 第三方SDK

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, 通过声明式的组件化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。
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 console s, 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 App Utils	Stumble App	一个简单的 React-Native Utils 库, 具有随机有用的功能。主要用于后台服务任务, 例如通知 onReceive 事件。

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.
-------------------------	--	---

🔑 密钥凭证

可能的密钥
友盟统计的=> "UMENG_CHANNEL" : "web"
友盟统计的=> "UMENG_APPKEY" : "676a78167e5e6a4eebc4dfe0"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"library_zxingandroidembedded_author" : "JourneyApps"

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