南明离火
移动应用检测平台

ANDROID 静态分析报告

BAM Crawford • v6.14.1

分析日期: 2025-08-26 11:42:58

应用概览

文件名称:	BAM Crawford v6.14.1.apk
文件大小:	77.3MB
应用名称:	BAM Crawford
软件包名:	com.customchurchapps.bamcm
主活动:	com.subsplash.thechurchapp.SplashActivity
版本号:	6.14.1
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:	49/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估：可能有安全隐患
MD5:	cdcf92da9b5faf40eedd1d87b1702b58
SHA1:	abf246be2fdf104abe4f474075921429514a1fba
SHA256:	375fd090fda37154487b1abd127fde262ec56bafbe78cb5378a28b5a91446ae

分析结果严重性分布

高危	中危	信息	安全	关注
3	25	4	2	0

四大组件导出状态统计

Activity组件：33个，其中export的有： 1个
Service组件：15个，其中export的有： 5个
Receiver组件：16个，其中export的有： 4个
Provider组件：11个，其中export的有： 1个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=US, ST=OR, L=Portland, O=Bible And Journal App LLC, OU=Development, CN=Poncho Lowder
签名算法: rsassa_pkcs1v15
有效期自: 2012-07-04 22:25:56+00:00
有效期至: 2062-06-22 22:25:56+00:00
发行人: C=US, ST=OR, L=Portland, O=Bible And Journal App LLC, OU=Development, CN=Poncho Lowder
序列号: 0x4ff4c2f4
哈希算法: sha1
证书MD5: 2e207f57b9cb62e20d728b43e24e02ad
证书SHA1: cfae439a68ed0515a78c832b8244482483ce7d5e
证书SHA256: 6285d339f2433376dbd3fc8f79bce0d52ab0cad463331d8e9087b72ec2039404
证书SHA512:
696d3d000668785424b96b31e48ebb5f52c23b43d047d60e4131c32a934f28277432bec034a8dc7d369b6d26bae233e2fc4b81e3554adc35ecdefc318667377

公钥算法: rsa
密钥长度: 1024
指纹: 868121c3b28d46001461512c1f49b3bfb35de87f5ce6a5620b58cbbffb4f930f
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.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.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.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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.READ_CONTACTS	危险	读取联系人信息	允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.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。
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.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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
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。
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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
com.customchurchapps.bamcm.permission.MAPS_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
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.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.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。
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。
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.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.customchurchapps.bamcm.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.subsplash.thechurchapp.DeepLinkActivity	Schemes: saphtf22n://, https://, Hosts: sap, bamcrawfordministries.subspla.sh,

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: **13** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F160006]	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。
2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Activity (com.subsplash.thechurchapp.DeepLinkActivity) 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。
4	Activity 设置了 TaskAffinity 属性 (com.subsplash.thechurchapp.media.MediaActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
5	Service (com.subsplash.thechurchapp.media.TrackMediaProgress) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
6	Service (com.subsplash.thechurchapp.api.PushIntentService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
7	Service (com.subsplash.thechurchapp.media.MediaPlaybackService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
8	Broadcast Receiver (com.subsplash.thechurchapp.media.MediaIntentReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
9	Content Provider (org.birkir.carplay.media.MediaArtworkContentProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。

10	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	检测到 Service 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。
11	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
12	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 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。
13	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。
14	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: **3** | 警告: **10** | 信息: **2** | 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	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
3	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
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	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	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
7	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
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	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

10	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
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
12	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
13	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
14	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
15	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
16	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
17	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

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。	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/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
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。	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', '__strncat_chk']	True 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。	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: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__strchr_chk']	True 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。	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

6	arm64-v8a/libjscinstance.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
7	arm64-v8a/libjserrorhandler.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

8	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']	True info 符号被剥离
9	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。	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

10	arm64-v8a/librninstance.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/librrc_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。	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

12	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。	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
13	arm64-v8a/librrc_native.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

14	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。	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
15	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。	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

16	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。	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
17	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。	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

18	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。	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
19	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。	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: ['__vsnprintf_chk']	True info 符号被剥离

20	arm64-v8a/libstatic-webp.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: ['__memcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info 符号被剥离
21	arm64-v8a/libuimanagerjni.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

本报告由南明离火移动安全分析平台生成

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

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
00013	读取文件并将其放入流中	文件	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
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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00147	获取当前位置的时间	信息收集 位置	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
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
00183	获取当前相机参数并更改设置	相机	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
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
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
00072	将 HTTP 输入流写入文件	命令 网络 文件	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
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
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
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

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
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
00012	读取数据并放入缓冲流	文件	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
00091	从广播中检索数据	信息收集	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
00192	获取短信收件箱中的消息	短信	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
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
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	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
00052	删除内容 URI 指定的媒体（SMS、CALLLOGS、文件等）	短信	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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00195	设置录制文件的输出路径	录制音视频 文件	升级会员：解锁高级权限
00007	Use absolute path of directory for the output media file path	文件	升级会员：解锁高级权限

00041	将录制的音频/视频保存到文件	录制音视频	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	9/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.RECEIVE_BOOT_COMPLETED android.permission.READ_CONTACTS android.permission.CAMERA android.permission.WAKE_LOCK android.permission.READ_CALENDAR android.permission.WRITE_CALENDAR android.permission.VIBRATE
其它常用权限	9/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID

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
status.subsplash.com	安全	否	**IP**地址: 18.238.243.116 国家: 荷兰（王国） 地区: 北荷兰省 城市: 阿姆斯特丹 纬度: 52.378502 经度: 4.899980 查看: Google 地图
pagead2.googlesyndication.com	安全	是	**IP**地址: 180.163.151.38 国家: 中国 地区: 上海 城市: 上海 纬度: 31.230416 经度: 121.473701 查看: 高德地图

t.subsplash.com	安全	否	**IP地址:** 100.21.19.64 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
goo.gl	安全	否	**IP地址:** 216.58.214.14 国家: 德国 地区: 黑森 城市: 美因河畔法兰克福 纬度: 50.110882 经度: 8.681996 查看: Google 地图
iptc.org	安全	否	**IP地址:** 3.64.29.21 国家: 德国 地区: 黑森 城市: 美因河畔法兰克福 纬度: 50.110882 经度: 8.681996 查看: Google 地图
feeds.subsplash.com	安全	否	**IP地址:** 100.21.19.64 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图
www.npes.org	安全	否	**IP地址:** 104.21.43.185 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
ns.useplus.org	安全	否	**IP地址:** 54.83.4.77 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
dashboard.thechurchapp.org	安全	否	**IP地址:** 199.60.103.31 国家: 美国 地区: 东京 城市: 波特兰 纬度: 45.523460 经度: -122.676468 查看: Google 地图

cipa.jp	安全	否	**IP地址:** 199.60.103.31 国家: 日本 地区: 东京 城市: to CamargoPorto CastilhoPorto Cervo Porto CesareoPorto Cheli Porto CovoPorto CristoPorto DiamantePorto Ercol 纬度: 35.689499 经度: 139.692322 查看: Google 地图
aomedia.org	安全	否	**IP地址:** 35.190.39.113 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
exoplayer.dev	安全	否	**IP地址:** 52.27.15.180 国家: 美国 地区: 宾夕法尼亚 城市: otteZASouth AfricaZMZambiaZWZimbabwe'Adan'Ajlun'Ajman'Amran'Asir'Eua-Akkar-AargauAbay oblysyAbiaAbidjan 纬度: 40.065647 经度: -79.891724 查看: Google 地图
www.aiim.org	安全	否	**IP地址:** 199.60.103.31 国家: 美国 地区: 马萨诸塞州 城市: 剑桥 纬度: 42.370129 经度: -71.086304 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
artwork.subsplash.com	安全	否	**IP地址:** 18.238.243.97 国家: 荷兰（王国） 地区: 北荷兰省 城市: 阿姆斯特丹 纬度: 52.378502 经度: 4.899980 查看: Google 地图
native-apps-225319.firebaseio.com	安全	否	**IP地址:** 35.190.39.113 国家: 美国 地区: 密苏里州 城市: 堪萨斯城 纬度: 39.099731 经度: -94.578568 查看: Google 地图

subsplash.wufoo.com	安全	否	**IP地址:** 18.238.243.8 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://help.dottoro.com/lcbixvwm.phparseFontStringetCanonicalLocalesPDFAcroFormissed • https://git.io/JflFv • https://subspla.sh/9d99f99https • https://www.sitepoint.com/css3-cursor-styles/sdk/ui_kit/configurationalsActivitiestrmoment • https://drafts.fxtf.org/css-masking-1 • https://github.com/csstree/stylelint-validator/issues/29 • https://images.subsplash.com/image.jpg?id=77c609f1-6307-4104-966b-ab51172065e2&w • https://docs.sentry.io/platforms/javascript/best-practices/browser-extensions/options/messages/mark_as_deliveredStateUpdate&filter • https://core.subsplash.com/end-user-auth/v1/auth-providers/19bc7532-7e56-440c-bd2e-171026dd5195/token?app_key=HTF22Nu0026origin_auth_provider=facebook • https://images.stage.subsplash.net/image.jpg?id=816e8e5f-5aec-4b19-b27e-1788c2029143&w • https://git.io/Jf4AR • https://react.dev/link/invalid-hook-call • http://help.dottoro.com/lcxquvkf.phparenthesesetTokenStatuseChatAuthorization • https://core.subsplash.com/end-user-auth/v1/auth-providers/19bc7532-7e56-440c-bd2e-171026dd5195/token?app_key=HTF22N • https://github.com/date-fns/date-fns/blob/master/docs/upgradeGuide.md • https://redux.js.org/Errors?code=&Acy • https://spotlightjs.com • https://images.subsplash.com/image.jpg?id=8a3b6e40-9cec-4783-af87-6a0f3e3af0425&w • https://images.subsplash.com/image.jpg?id=81a02c5-6803-4c84-915b-876f6156405f&w • http://momentjs.com/timezone/docs • https://t.subsplash.com/api/v1/HTF22N/app_metrics • https://feeds.subsplash.com/api/v1/topic-subscriptions/HTF22N • https://t.subsplash.com/callback/HTF22N • https://onvdmt2jxd.execute-api.us-west-2.amazonaws.com/default/fetchBibleContentAndSaveToDevice • https://images.subsplash.com/image.jpg?id=5d7cdb-d1f3-4610-8133-17b8832326da&w • https://github.com/date-fns/date-fns/blob/master/docs/unicodeTokens.mdpig_nosendPlayPosition • https://feeds.subsplash.net/api/v1/event-detail/d80bc7b4-26fb-42ec-8833-2ba65baa6afbaseLodashWrapperPercentageOrAbsoluteLengthPlusKeywordsetVisibleflag-globalHandlerLog • http://jmrog2.net/tmp/canvas_image_zoom.htmlStartTagInBodyflag-http.request.domain_lookup_endTagOutsideForeignContentriggerUserActivityflag-idistanceFromStartflag-ieflag-ilocaleErasParseeProsetteflag-initMediaInteractionObserveremoveFieldflag-iqhandleLoadedoubleClickYflag-irefundedflag-is • https://assets.static.subsplash.com/fonts/proxima-nova/bold/ProximaNova-Bold-webfont.woff2 • https://spotlightjs.com/sidecar/npx/operatorsameAsMarginitStyleDeclarationObserveremoveHighlightedAndSaveToDevice_dedupeIntegrationScrollShouldSetResponderCapturecently_added • http://momentjs.com/guides • https://images.subsplash.com/image.jpg?id=80399b36-97a1-4b73-81e5-4db6509cc4bc&w • https://t.subsplash.com/api/v1/redirect • https://assets.static.subsplash.com/fonts/proxima-nova/regular/ProximaNova-Reg-webfont.woff2 • https://react.dev/link/refs-must-have-owner	

- https://images.subsplash.com/image.jpg?id=aa141b63-4362-4d87-b74b-c2db234cb72b&w
- https://core.subsplash.com/end-user-auth/v1/auth-providers/f8b7f2ad-09e1-4a73-ba1b-27da82ac8052/token?app_key=HTF22N
- https://feeds.subsplash.com/api/v1/manifest/HTF22N
- https://github.com/styled-components/styled-components/blob/master/packages/styled-components/src/utils/errors.md
- https://spacex.comboboxShadowrapWithConnectAdvanced
- https://docs.swmansion.com/react-native-gesture-handler/docs
- https://github.com/csstree/csstree/issues
- https://www.interbaycc.com/contact_emailhttps
- https://images.subsplash.com/image.jpg?id=59f9feb9-9da4-42fa-96ed-b77c932acb5c&w
- https://images.subsplash.com
- https://feeds.subsplash.com/api/v1/structure/HTF22N
- http://help.dottoro.com/lcrthhhv.phpar
- https://stripe.com/docs/stripe-js/react
- https://images.unsplash.com/photo-1446776811953-b23d57bd21aa?ixlib=rb-1.2.1&ixid=eyJhcHBfaWQiOjEyMDd9&auto=format&fit=crop&w=800&q=60https
- https://bugzilla.mozilla.org/show_bug.cgi?id=947588KitInputPreviewIsDescendantOflag-asSpecifiedWithLengthsAbsoluteAndNormalComputingToZeroExceptMultiColumnCombinator
- https://docs.sentry.io/platforms/react-native/troubleshooting
- https://images.subsplash.com/image.jpg?id=2cf83812-3c7b-4141-bccb-d2e3e1174e6a&w
- http://help.dottoro.com/lclhnthl.phpalms_up_togethermesStacksfetchDatadded
- https://feeds.dev.subsplash.net/api/v1/profile/8GX4XH/user-infoLog
- https://github.com/mdn/data/pull/431
- https://images.dev.subsplash.net
- https://images.subsplash.com/image.jpg?id=cf5aadbd-abe7-4242-b948-96a884f[illegible]&w
- https://github.com/Hopding/pdf-lib
- https://images.subsplash.com/image.jpg?id=6d797d7b-a608-4747-a8ef-6e2[illegible]0956e&w
- https://secure.subsplash.com/ui/access/HTF22N
- https://images.subsplash.com/image.jpg?id=715e4db8-9129-4a20-b[illegible]f8-[illegible]70e596136&w
- https://momentjs.com/timezone/docs
- https://sentry.io/welcome/relatedByScripturemoveFormatTrackJpkensureIsTagetFunctionNamehttps
- https://assets.static.subsplash.com/fonts/proxima-nova/extra-bold/ProximaNova-ExtraBold-webfont.woff2
- https://feeds.subsplash.com/v2/sessions/HTF22N
- https://github.com/lahmatiy
- http://sourceforge.net/adobe/aglfn
- http://fb.me/use-check-prop-typesAreEqualCSSFontFeatureValuesRuleHarpoondownharpoonleftarrow-menu-leftButtonStyleCSSKeyframeRuleftrightsquigarrow_up_small_blue_diamondCSSKeyframesRulegacyLiveChatRouteCSSOM
- https://feeds.subsplash.com/api/v1/platform-endpoints/HTF22N
- https://js.stripe.com/v3
- https://native-web.subsplash.com/search
- https://core.subsplash.com/end-user-auth/v1/auth-providers/19bc7532-7e56-440c-bd2e-171026dd5195/authorize?app_key=HTF22N
- https://www.bamcm.org
- https://subsplash.com/sunny/appUpdatePromptLoginModallowFriendDiscoveryProv.Provide
- https://stackoverflow.com/questions/14343965/google-places-library-without-map
- https://feeds.subsplash.com/api/v1/states
- https://play.google.com/store/apps/details?id=com.customchurchapps.bamcm
- https://core.subsplash.com/end-user-auth/v1/auth-providers/19bc7532-7e56-440c-bd2e-171026dd5195/authorize?app_key=HTF22Nu0026origin_auth_provider=facebook
- https://twitter.com/intent/tweet?url=https
- https://images.subsplash.com/image.jpg?id=c1e4dfb8-f6bb-4d28-8611-ea56cd88bcaf&w
- http://help.dottoro.com/lcbkewgt.phparseFormatStrack-media-progressViewOffsetupFormatInfocusedControl_isDismissed
- https://react.dev/link/strict-mode-string-refEqualitycompilePath
- https://feeds.subsplash.com/api/v1
- https://feeds.subsplash.com/api/v1/profile/CHURCH/users/mute/messages/changelogsame-originalColumnhttps
- https://core.subsplash.com/end-user-auth/v1/auth-providers/f8b7f2ad-09e1-4a73-ba1b-27da82

自研引擎-A

ac8052/authorize?app_key=HTF22N	
• http://dashif.org/guidelines/trickmode • http://dashif.org/guidelines/last-segment-number • data:cs:audiopurposecs:2007	pb/c.java
• http://dashboard.thechurchapp.org/platform/feeds/schemas/ipad_double/ • http://dashboard.thechurchapp.org/platform/feeds/schemas/double/ • http://dashboard.thechurchapp.org/platform/feeds/schemas/ipad/	com/subsplash/thechurchapp/handlers/more/a.java
• https://status.subsplash.com/	com/subsplash/thechurchapp/dataObjects/ConnectionBarData.java
• 10.0.1.1	i8/b.java
• https://aomedia.org/emsg/id3 • https://developer.apple.com/streaming/emsg-id3	eb/a.java
• https://artwork.subsplash.com/images/cdn/%s/%d/%d/ios/circle.png	com/subsplash/thechurchapp/handlers/app/AppHandler.java
• https://plus.google.com/	ed/u1.java
• http://dashboard.thechurchapp.org/platform/feeds/schemas/double/	com/subsplash/thechurchapp/handlers/table/a.java
• http://dashboard.thechurchapp.org/platform/feeds/schemas/ipad_double/ • http://dashboard.thechurchapp.org/platform/feeds/schemas/double/ • http://dashboard.thechurchapp.org/platform/feeds/schemas/ipad/	com/subsplash/thechurchapp/handlers/table/c.java
• http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java
• http://purl.org/rss/1.0/modules/content/	com/subsplash/thechurchapp/handlers/rss/c.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• http://%s/inspector/device?name=%s&app=%s&device=%s	m8/d.java
• https://%s/%s/%s	eg/c.java
• https://exoplayer.dev/issues/player-accessed-on-wrong-thread	ia/c2.java
• http://dashboard.thechurchapp.org/platform/feeds/schemas/ipad_double/ • http://dashboard.thechurchapp.org/platform/feeds/schemas/double/ • http://dashboard.thechurchapp.org/platform/feeds/schemas/ipad/	com/subsplash/thechurchapp/handlers/detail/a.java
• https://exoplayer.dev/issues/cleartext-not-permitted	gc/w.java
• http://dashboard.thechurchapp.org/platform/feeds/schemas/double/	com/subsplash/thechurchapp/handlers/playlist/PlaylistParser.java
• http://goo.gl/8rd3yj	wd/s.java

本报告由南明离火移动安全分析平台生成

• 10.0.3.2 • 10.0.2.2	x8/a.java
• http://goo.gl/8rd3yj	wd/d1.java
• https://accounts.google.com/o/oauth2/revoke?token=	qc/f.java
• http://www.aiim.org/pdfa/ns/property# • http://cipa.jp/exif/1.0/ • http://iptc.org/std/iptc4xmpcore/1.0/xmlns/ • http://iptc.org/std/iptc4xmpext/2008-02-29/ • http://www.aiim.org/pdfa/ns/schema# • http://www.aiim.org/pdfa/ns/type# • http://www.aiim.org/pdfa/ns/field# • http://www.aiim.org/pdfa/ns/extension/ • http://www.aiim.org/pdfa/ns/id/ • http://ns.useplus.org/ldf/xmp/1.0/ • http://www.npes.org/pdfx/ns/id/	u1/p.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	kc/b.java
• http://javax.xml.xmlconstants/feature/secure-processing	u1/l.java
• https://subsplash.wufoo.com/forms/feedback/def/field139=%s • https://t.subsplash.com/callback/%s/ • https://feeds.subsplash.com/v3/setup/{{app_key}}	com/subsplash/thechurchapp/api/h.java
• https://native-apps-225319.firebaseio.com	自研引擎-S
• file:line	lib/arm64-v8a/libglog.so

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://native-apps-225319.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL（https://firebaseremoteconfig.googleapis.com/v1/projects/608610324/namespaces/firebase:fetch?key=AIzaSyCR7RGPlXaBT8ucv21tLVQnM7FSBcTqvQw）已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

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 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.
Sentry	Sentry	Sentry 是一个实时事件日志记录和聚合平台，它专门用于监视错误和提取执行适当的事后操作所需的所有信息。
uCrop	Yalantis	Android 图片裁剪库
Jetpack Car	Google	Build navigation and point of interest apps for Android Auto and Android Automotive OS.
Google Sign-In	Google	提供使用 Google 登录的 API。
Google Play Service	Google	帮助 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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Google Analytics	Google	提供各种 API，可帮助您收集、配置和报告用户与您的在线内容进行互动的数据。
Google Cast	Google	使用 Google Cast SDK，您可以扩展 Android，iOS 或 Chrome 应用，以将其流式视频和音频定向到电视或声音系统。 您的应用程序成为播放，暂停，搜索，倒带，停止和控制媒体的遥控器。

Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

邮箱地址敏感信息提取

EMAIL	源码文件
support@subsplash.com	com/subsplash/thechurchapp/DebugActivity.java

第三方追踪器检测

名称	类别	网址
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.google.android.geo.API_KEY" : "AIzaSyAIbpdmzkOrNz79Z7TLN_h6BCMZ3CLwqsg"
Google_Drive_API_Key: AIzaSyAIbpdmzkOrNz79Z7TLN_h6BCMZ3CLwqsg AIzaSyCt7VX6RL35nrFxgWks2K4Akg9coeVxt7E
"firebase_database_url" : "https://native-apps-225319.firebaseio.com"
"google_api_key" : "AIzaSyCR7RGPlXaBT8ucv21tLVQnM7FSBcTqvQw"
"google_app_id" : "1:608610314:android:d05583746275f260"
"google_crash_reporting_api_key" : "AIzaSyCR7RGPlXaBT8ucv21tLVQnM7FSBcTqvQw"
8138e8a0fcf3a4ce4a971d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86f5a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
AIzaSyBJnJdMyCm9NZwtStaUHWHB4SVR7bdevi0
19bc7532-7e56-440c-bd2e-171026dd5195
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

Google Play 应用市场信息

标题: BAM Crawford Ministries

评分: 4.875 安装: 1,000+ 价格: 0 **Android**版本支持: 分类: 生活时尚 **Play Store URL:** com.customchurchapps.bamcm

开发者信息: Subsplash Inc, Subsplash+Inc, None, https://www.subsplash.com/, appsupport@subsplash.com,

发布日期: 2021年8月5日 隐私政策: Privacy link

关于此应用:

这是 BAM Crawford 事工和国际圣经丰富团契教会 (B.E.F.I.C.) 的官方应用程序，由创始人/资深牧师贝弗利·“BAM”·克劳福德 (Beverly "BAM" Crawford) 牧养。 BAM 使徒蒙神恩典，成为神国度中一位完美的先知教师。近 45 年来，她一直致力于公共服务，跨越国家、民族和文化，为人们带来全面而透彻的圣经启示。 与事工建立联系变得更容易！只需轻轻一点，即可访问：• 视频和音频讲道 • 直播 • 电子商店 • BAM Crawford 宗旨音乐 • 读经计划 • 活动 • 代祷事项等等 下载并享受内容后，您可以通过 Facebook、Twitter、Instagram 或电子邮件与家人和朋友分享。在 BAM Crawford 事工，人们彼此联系，家庭成长，生命因耶稣基督被高举而改变。 Apostle 最喜欢的名言是：“好，更好，最好，永不停歇，直到你的好变得更好，你的好变得更好”。移动应用版本：6.15.1

免责声明及风险提示: