南明离火
移动应用检测平台

ANDROID 静态分析报告

Sushain

sushain • v0.0.42

分析日期: 2025-08-01 13:16:24

应用概览

文件名称:	sushain.apk
文件大小:	20.0MB
应用名称:	sushain
软件包名:	com.sushain.marketplace
主活动:	com.sushain.marketplace.MainActivity
版本号:	0.0.42
最小SDK:	23
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:	59/100 (中风险)
跟踪器检测:	1/432
杀软检测:	1 个杀毒软件报毒
MD5:	3937c3205e7ce4808db41844644ed378
SHA1:	3242a3ae8113163[illegible]d0cb4fd9ada34b951f
SHA256:	c1b66b6823d[illegible]d6793f22a155a8a667caae715a40a2da7c3ec0814d911a7

分析结果严重性分布

高危	中危	信息	安全	关注
1	13	3	3	0

四大组件导出状态统计

Activity组件：2个，其中export的有：0个
Service组件：11个，其中export的有：1个
Receiver组件：5个，其中export的有：3个
Provider组件：8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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2024-04-21 21:19:46+00:00
有效期至: 2054-04-21 21:19:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xb1a87428f5cb1b3731378c12f0caba97b76a0217
哈希算法: sha256
证书MD5: 0107d34cea8ee021136247f53bf43789
证书SHA1: 0d9e2a03f4d6c0556703a055ec0f7c2ae6ea1acc
证书SHA256: e5dfae2f35c98075057bbb2a8c19cf946ce7d1fab06e60ec089f847f4031dd40
证书SHA512:
355df3aaa5f1ea6ee5e8d361514af6894c193df36d1483947a03ed6a22d81404233bd0e966967f28f6e16cc91778cb565f11d4627b903...28ee6bb2ab0fbf2ff

公钥算法: rsa
密钥长度: 4096
指纹: 1dd1d070811d0774df800600d590c0b25005fa65485b1817e715612f07084cdc
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.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.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
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.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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
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.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。

android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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.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。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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.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。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
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。
android.permission.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
com.sushain.marketplace.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.android.vending.CHECK_LICENSE	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	严重级别	描述

证书安全合规分析

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: **5** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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。
3	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。
4	Broadcast Receiver (com.cashfree.pg.core.api.ui.receiver.CFSMSBroadcastReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.phone.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。
5	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。

代码安全漏洞检测

高危: **1** | 警告: **6** | 信息: **3** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置

1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
3	应用程序使用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	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
5	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
6	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
7	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
8	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
9	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

10	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
11	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
12	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

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
00056	修改语音音量	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
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00043	计算WiFi信号强度	信息收集 WiFi	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	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
00102	将手机扬声器设置为打开	命令	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
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
00013	读取文件并将其放入流中	文件	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
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
00208	捕获设备屏幕的内容	信息收集 屏幕	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00085	获取ISO国家代码并将其放入JSON中	信息收集 电话服务	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	7/30	android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO android.permission.SYSTEM_ALERT_WINDOW android.permission.WAKE_LOCK

其它常用权限	12/46	android.permission.READ_MEDIA_IMAGES android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
shopify.github.io	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
payments-test.cashfree.com	安全	否	**IP地址:** 43.204.88.167 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
payments.cashfree.com	安全	否	**IP地址:** 18.238.243.9 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
sandbox.cashfree.com	安全	否	**IP地址:** 3.109.101.46 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图

api.cashfree.com	安全	否	**IP地址:** 13.227.219.22 **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
www.cashfree.com	安全	否	**IP地址:** 18.239.36.120 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378508 **经度:** 4.899980 **查看:** Google 地图
docs.swmansion.com	安全	否	**IP地址:** 104.21.27.136 **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
receiver.cashfree.com	安全	否	**IP地址:** 18.238.243.9 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
cashfreelogo.cashfree.com	安全	否	**IP地址:** 18.238.243.9 **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

• https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting • https://react-spectrum.adobe.com/react-aria/useMove.htmlDecodeTreeborderBottomStartRadiuseFiberelayoutFromIndexborderEndEndRadiuseFocusEventsigBytesborderStartEndRadiuseFocusedListenersChildrenAdaptereload-circle-sharprepareAutoBatchedborderTopStartRadiuseGetCitiesByStateIrcornerRadiuseGetCompletedAppointmentsignInNowithoutDefaultFocusAndBlurcurrentBorderRadiuseGetDoctorBookedSlotsignInSilentlyfetchStatuseGetDoctorBySpeclizationInlineViewLayoutgetNextHandlerTagetAuthorizationStatuseGetDoctorLanguagestureDirectionativeExtensionsgetUpdateStatuseGetDoctorsAllSlotsignOutinstallStatuseGetFindADoctorSelectedmapPropsToStatuseGetInstantDoctorsBySpeclizationInputFocustomAnimationOnSwipeerConnectionInitcloud-offline-sharpadRadiuseGetMedicinesComboslasharedAction_producerstepStatuseGetOrderLastMinByvalidateStatuseGetReportByAppointmentId_locateFirstNeighbourIndexopluseGetSearchProductsByNamedicineCart2useIMGNormalizedSourceuseImageConcreteDimensionsignalListeneruseImageNaturalDimensionsignalingStateuseInteractOutsidebugLogenerateNewNodeTagetApplicationNameuseInteractionModalityuseIsKeyboardShownKeysuseIsomorphicLayoutEffectWithArgsilentJSONParsingetDescendantStyleIdsuseKeyedChildListenersilveruseLatestCallbackTitleVisibleuseLinkingContextShadowOffsetDtlsRoleuseLongPressl-SIGN_IN_CANCELLEDuseMediaQueryuseMergeRefslarrtlMarkerReverseduseNavigationHelpersContextTransformatRangeToPartsuseOnActionInsertuseOnGetStateuseOnPreventRemoveProviderenderSuffixuseOptionsGettersliceCaseReducersByNameuseOrderAddressUpdateuseOrderCartCreateuseOrderCreateuseParentSafeAreaFrameContextendedConfigetAllowedDropOperationsuseParentSafeAreaInsetsContextension-puzzle-outlineusePatchesInScopenLeftusePortalProvidereload-outlineusePressStateusePresseduseProfilereload-sharprepareDataForValidationparallelLatencyThrottleMsuseReduxContext2useRefEffectotal_packets_lost_outuseResizeObserverboseStyledInputSlotUnmountableHandleStartShouldSetResponderuseScheduleUpdateContextension-puzzle-sharparseFeeduseScrollWheelementTypeerConnectionSetConfigurationotifyTaskFinisheduseSelector2useSheetManageremideBtnStyleuseStore2useSymbolicMarkerRendererPropsliceCaseReducersByTypeuseSyncStateuseTTreeChangeEffectotal_packets_outuseTotalColumnFlexit-outlineOmicronMouseUpdateEffectotal_pli_received_outuseUserRegisteremindLateruseValueEffectotal_removed_samples_for_accelarationuseViewportSizeuseVisuallyHiddenableAccessToHostTreeInFabriconColoruseandom-26T198340PX75pxJACKVERYMINDBUSHWOLF_GQZbfghjklqvwyzrictotal_rtt_connectivity_measureCallbackdropOpacity_pausedReactProfileremoteCandidateIdUserLocalAddressliceMatchersuser_engagementotal_rtt_ms_outuuuuidv4_autoplayInterval • http://invertase.link/android • https://bit.ly/3cXEKWfilterModefaultRetryDelayoutChanget • http://invertase.link/ios • http://fb.me/use-check-prop-types/index.d.tshowRightAction • https://react.dev/link/strict-mode-string-ref • https://dev.to/li/how-to-requestpermission-for-devicemotion-and-devicerorientation-events-in-ios-13-46g2.30.1.84usePreviously • https://react.dev/link/refs-must-have-owner • https://docs.swmansion.com/react-native-reanimated/docs/fundamentals/glossary • https://www.cashfree.com • https://react.dev/link/invalid-hook-call • http://momentjs.com/guides • https://docs.swmansion.com/react-native-gesture-handler/docs • https://redux-toolkit.js.org/Errors?code • https://redux.js.org/Errors?code=_getCustomDataLengthandleStrictParse • https://github.com/adobe/react-spectrum/issues/2320We	自研引擎-B
• https://receiver.cashfree.com/pgnextgenconsumer/analytics/external/v1/android/ • https://payments.cashfree.com/pgbillpayuiapi/exceptions/sentry/v1/androidparsedatatosentry/ • https://payments-test.cashfree.com/pgbillpayuiapi/exceptions/sentry/v1/androidparsedatatosentry/	com/cashfree/pg/cf_analytics/network/CFLoggingRequest.java
• https://api.cashfree.com/pg/ • https://receiver.cashfree.com/pgnextgenconsumer/ • https://sandbox.cashfree.com/pg/ • https://sandbox.cashfree.com/pgnextgenconsumer/	com/cashfree/pg/core/hidden/utils/URLConstants.java

• https://api.cashfree.com/pg// • https://payments.cashfree.com/order/icons/ • https://cashfreelogo.cashfree.com/assets_images/pg/ • https://sandbox.cashfree.com/pg/	com/cashfree/pg/ui/hidden/utils/URLConstants.java
• https://cashfreelogo.cashfree.com/assets_images/pg/wallet/%s%s.png	com/cashfree/pg/ui/hidden/utils/WalletImageUrl.java
• https://cashfreelogo.cashfree.com/assets_images/pg/paylater/%s%s.png	com/cashfree/pg/ui/hidden/utils/PayLaterImageUrl.java
• https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting#java-side-failed-to-resolve-c-code-version • https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting#mismatch-between-java-code-version-and-c-code-version	com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java
• https://cashfreelogo.cashfree.com/assets_images/pg/nb/%s%s.png	com/cashfree/pg/ui/hidden/utils/BankImageUrl.java
• https://api.cashfree.com/pg/ • https://receiver.cashfree.com/pgnextgenconsumer/ • https://sandbox.cashfree.com/pg/ • https://sandbox.cashfree.com/pgnextgenconsumer/	com/cashfree/pg/core/BuildConfig.java
• https://api.cashfree.com/pg// • https://sandbox.cashfree.com/pgnextgenconsumer/ • https://receiver.cashfree.com/pgnextgenconsumer/ • https://sandbox.cashfree.com/pg/	com/cashfree/pg/ui/BuildConfig.java
• https://shopify.github.io/flash-list/docs/usage#cellrenderercomponent	com/shopify/reactnative/flash_list/AutoLayoutView.java
• https://api.cashfree.com/pg/ • https://sandbox.cashfree.com/pg/	com/cashfree/pg/core/hidden/network/request/FetchSavedCardsNetworkRequest.java
• https://api.cashfree.com/pg/ • https://sandbox.cashfree.com/pg/	com/cashfree/pg/core/hidden/network/request/DeleteSavedCardsNetworkRequest.java
• https://api.cashfree.com/pg/ • https://sandbox.cashfree.com/pg/	com/cashfree/pg/core/api/ui/CFWebView.java
• https://sandbox.cashfree.com/pgnextgenconsumer/order/external/android/config? • https://receiver.cashfree.com/pgnextgenconsumer/order/external/android/config?	com/cashfree/pg/core/hidden/network/request/ConfigNetworkRequest.java
• https://sandbox.cashfree.com/pg/orders/sessions/app • https://api.cashfree.com/pg/orders/sessions/app	com/cashfree/pg/core/hidden/network/request/BaseNetworkRequest.java
• https://www.cashfree.com/ • https://payments.cashfree.com/	com/cashfree/pg/core/api/ui/BaseCFWebView.java
• https://sandbox.cashfree.com/pg/orders/pay/authenticate/ • https://api.cashfree.com/pg/orders/pay/authenticate/	com/cashfree/pg/core/hidden/network/request/NativeSubmitOTPRequest.java

本报告由南明离火移动安全分析平台生成

• https://sandbox.cashfree.com/pg/orders/pay/authenticate/ • https://api.cashfree.com/pg/orders/pay/authenticate/	com/cashfree/pg/core/hidden/network/request/NativeResendOTPRequest.java
• https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• https://api.cashfree.com/pg/ • https://sandbox.cashfree.com/pg/	com/cashfree/pg/core/hidden/network/request/RecentNetworkRequest.java
• https://sandbox.cashfree.com/pgnextgenconsumer/ • https://receiver.cashfree.com/pgnextgenconsumer/	com/cashfree/pg/core/hidden/network/request/OrderStatusNetworkRequest.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/996922397465/namespaces/firebase:fetch?key=AIzaSyCKsfRx7AMLR2PWLMdp8WdV9lIBQS1z9E8 ） 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
Google Sign-In	Google	提供使用 Google 登录的 API。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
Process Phoenix	JakeWharton	Process Phoenix facilitates restarting your application process.
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。

Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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 AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

第三方追踪器检测

名称	类别	网址
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
Google_Drive_API_Key: AIzaYRtRtcBO3li1bTlLBjE6CoIkt6A02wgXrDV
"google_api_key" : "AIzaSyCKsFRx7AMLR2PWLMdp8WdV9lIBQS1z9E8"
"google_app_id" : "1:996922397465:android:e1d9a2681f72bfea02b88"
"google_crash_reporting_api_key" : "AIzaSyCKsFRx7AMLR2PWLMdp8WdV9lIBQS1z9E8"
aXNccyhcZHs2LDh9KXwoXGR7Niw4fSlcc2lzfGlzXNMMbXGR7NH0p
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
bb392ec0-8d4d-11e0-a896-0002a5d5c51b

Google Play 应用市场信息

标题: Sushain

评分: 3.4153845 **安装:** 5,000+ **价格:** 0 **Android版本支持:** **分类:** 健康与健身 **Play Store URL:** com.sushain.marketplace

开发者信息: sushain wellness, sushain+wellness, None, https://sushainclinic.com, care@sushainclinic.com,

发布日期: 2024年5月31日 **隐私政策:** Privacy link

关于此应用:

欢迎来到 Sushain，您的终极医疗保健伴侣！通过无缝视频咨询，在舒适的家中与最好的顺势疗法和阿育吠陀医生联系。体验根据您的健康需求量身定制的个性化护理和专家建议。 有了 Sushain https://www.youtube.com/watch?v=lxFSHjNyeWk&t=6s，就可以轻松获得药物。浏览您值得信赖的医生开出的各种药物，然后只需轻按几下即可订购。享受送货上门服务，更加方便。 主要特征： 视频咨询：预约著名的顺势疗法和阿育吠陀医生，以获得详细的咨询和治疗计划。专家建议：从经验丰富的从业者那里获得个性化的健康建议和建议。 数字处方：咨询后获取数字处方，以便快速、轻松地购买药品。 药品订购：直接从应用程序浏览和购买处方药。 送货上门：在您方便的时候享受药品送货上门服务。 无论您寻求整体治疗还是专家医疗建议，Sushain 都能为您带来触手可及的医疗保健服务。今天就与 Sushain 一起掌控您的健康并开始您的健康之旅！ 立即下载 Sushain 应用程序，体验医疗保健的未来。

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。