南明离火
移动应用检测平台

ANDROID 静态分析报告

アザス • v1.5.2

分析日期: 2025-07-05 13:51:25

应用概览

文件名称:	com.azas v1.5.2.apk
文件大小:	10.53MB
应用名称:	アザス
软件包名:	com.azas
主活动:	com.azas.MainActivity
版本号:	1.5.2
最小SDK:	28
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:	55/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	23b359dda5042e7f60ec89e50c0cbd82
SHA1:	95186092c411b4f62f83959a1a6a668dd039ffe8
SHA256:	8f236e5d6492824d7d486e875dfb7c6be1b7d819f3700b7ee53105d91f5282c

分析结果严重性分布

高危	中危	信息	安全	关注
1	14	1	2	0

四大组件导出状态统计

Activity组件：5个，其中export的有： 1个
Service组件：4个，其中export的有： 2个
Receiver组件：15个，其中export的有： 4个
Provider组件：7个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: False
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: 2022-09-15 03:10:08+00:00
有效期至: 2052-09-15 03:10:08+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x4e61083e3e0255c91cede659a2bda3a44d289963
哈希算法: sha256
证书MD5: e81e0e1703fa0be2db16827b689522b8
证书SHA1: 19802daff28679bcab75a2c70106876f9e513270
证书SHA256: 1232b6f51a082f3371c9194f8cc8aef2817f0a2d41c7790d9d5710f5b65d9d8a
证书SHA512:
a84c4cd65d8c2b342883bf34f4866fbff34413c3d8fabbf3c3fb34ee35c4c726b98d8b1fae647bf20d5d8546816 4f0b44c26e7a43f8bb8 bdc29e27c483df

公钥算法: rsa
密钥长度: 4096
指纹: e3ce2ccfa4d151d2efdefe2eaf3cfbc46e80eb23c2575e4684472454049b9eff
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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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.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_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。
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。

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.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.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.azas.MainActivity	Schemes: azas://, Hosts: com.jgc.azas,

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: **7** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

1	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。
2	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。
3	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。
4	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。
5	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。
6	Activity (app.notifee.core.NotificationReceiverActivity) 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。

7	Broadcast Receiver (app.notifee.core.AlarmPermissionBroadcastReceiver) 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。

代码安全漏洞检测

高危: **1** | 警告: **6** | 信息: **1** | 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	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
6	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

7	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
8	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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
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
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
00031	检查当前正在运行的应用程序列表	反射 信息收集	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
00024	Base64解码后写入文件	反射 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
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
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
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
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
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
00091	从广播中检索数据	信息收集	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
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
00043	计算WiFi信号强度	信息收集 WiFi	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00002	打开相机并拍照	相机	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
00028	从assets目录中读取文件	文件	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	6/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED

其它常用权限	8/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE com.google.android.c2dm.permission.RECEIVE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NOTIFICATION_POLICY

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
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
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
e3f6979135e34ea0babd0a4eedb22cbc.apm.us-west-2.aws.cloud.es.io	安全	否	**IP地址:** 44.232.228.214 **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
notifee.app	安全	否	**IP地址:** 63.176.8.218 **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
www.aiim.org	安全	否	**IP地址:** 44.232.228.214 **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

cipa.jp	安全	否	**IP地址:** 118.82.81.189 国家: 日本 地区: 东京 城市: 东京 纬度: 35.689499 经度: 139.692322 查看: Google 地图
app.azas-token.com	安全	否	**IP地址:** 108.138.246.60 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 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
api.azas-token.com	安全	否	**IP地址:** 57.181.139.134 国家: 日本 地区: 东京 城市: 东京 纬度: 35.689499 经度: 139.692322 查看: Google 地图
static.azas-token.com	安全	否	**IP地址:** 108.139.10.44 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图

URL 链接安全分析

URL信息	源码文件

• http://phrogz.net/tmp/canvas_image_zoom.htmlocalizationDidChanget • http://help.dottoro.com/lcxquvkf.phparseComparatoreduce-capacityadd-photo-alternate-email-addressCityAndStateal500proxyTokenListreet-addressStateal600adjacentralConfigetLabelAngleborderTopStartRadiuseQuery • https://github.com/lahmatiy • https://github.com/csstree/stylelint-validator/issues/29 • http://help.dottoro.com/lcbkewgt.phparseFileHostringTicksno-meeting-roomissed • https://github.com/callstack/react-native-slider-movedurationMsRCTSwitchainedCheckTypeg • https://drafts.fxtf.org/css-masking-1 • https://docs.swmansion.com/react-native-reanimated/docs/fundamentals/installation • https://github.com/software-mansion/react-native-reanimated.github • https://github.com/csstree/csstree/issues • http://help.dottoro.com/lclhnthl.phparseCannotBeABaseURLPathexColoreactivateTimeoutadded • https://bugzilla.mozilla.org/show_bug.cgi?id=947588music-video-label-offirestoreDeletedValuesInNestedArraynot-listed-location-offirstLetterPseudoElementsAndInlineLevelFirstChildrenderCrosslicesheadset-mic-external-offirstRoutehttps • http://invertase.link/ios • http://invertase.link/android • http://help.dottoro.com/lcrthhhv.phparseChromeadded • https://github.com/mdn/data/pull/431 • http://help.dottoro.com/lcbixvwm.phparseEventReturncoreadNumberelativeTimemultilineFlexContainershouldUseNativeValidationativeEnumissed • https://www.sitepoint.com/css3-cursor-styles/Users/sakaguchi/Desktop/workspace/azas/TokenEconomy-app/node_modules/react-native-reanimated/src/reanimated2/Bezier.ts • http://fb.me/use-check-prop-typeslint	音研引擎-A
• https://static.azas-token.com • https://e3f69791358e4ea0ba0d0a4eedb22cbc.ap-northeast-1.aws.found.io:9243 • https://api.azas-token.com • https://app.azas-token.com	com/azas/BuildConfig.java
• https://accounts.google.com/o/oauth2/revoke?token=	o7/f.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
• 10.0.1.1	t5/b.java
• https://%s/%s/%s	fa/c.java
• https://notifee.app/react-native/docs/triggers#android-12-limitations	g1/m0.java

• http://javax.xml.xmlconstants/feature/secure-processing	l1/l.java
• http://www.aiim.org/pdfa/ns/type# • http://www.npes.org/pdfx/ns/id/ • http://iptc.org/std/iptc4xmpext/2008-02-29/ • http://www.aiim.org/pdfa/ns/schema# • http://ns.useplus.org/ldf/xmp/1.0/ • http://www.aiim.org/pdfa/ns/id/ • http://www.aiim.org/pdfa/ns/extension/ • http://www.aiim.org/pdfa/ns/property# • http://www.aiim.org/pdfa/ns/field# • http://iptc.org/std/iptc4xmpcore/1.0/xmlns/ • http://cipa.jp/exif/1.0/	l1/p.java
• https://static.azas-token.com • https://e3f6979135e34ea0babd0a4eedb22cbc.apm.us-west-2.aws.cloud.es.io:443 • https://api.azas-token.com • https://app.azas-token.com	自研引擎-S

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/970676142245/namespaces/firebase:fetch?key=AIzaSyBB27JdKQp5rIn_zjbCALphSddAQlA8YuI ）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。
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 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。

敏感凭证泄露检测

可能的密钥
"API_URL" : "https://api.azas-token.com"
"google_api_key" : "AIzaSyBB27JdKQp5rIn_zjbCALphSddAQlA8YuI"
"google_app_id" : "1:970676142245:android:1012a97c4b73db95228d4c"
"google_crash_reporting_api_key" : "AIzaSyBB27JdKQp5rIn_zjbCALphSddAQlA8YuI"
1ddaa4b892e61b0f7010597ddc582ed3
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
e3f6979135e34ea0babd0a4eedb22cbc
24b2477514809255df232947ce7928c4

Google Play 应用市场信息

标题: アザス - 建設現場の活性化と安全文化の実現

评分: None **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 办公 **Play Store URL:** com.azas

开发者信息: JGC Digital K.K., JGC+Digital+K.K., None, None, azas.app@jgc.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

“Azasu”是一款智能手机应用程序，通过赞扬主管希望鼓励工作现场工人的日常良好行为（好行动）来促进主管和工人之间的沟通，并支持实现安全现场操作。它是基于 JGC 集团现场的专业知识开发的，该集团在日本和海外运营着众多建筑工地，以确保安全施工。除了“点赞”之外，它还具有将现场发生的险情报告并现场公开的功能，以及兑换现场设置的奖品的功能。 当您离开现场或工作结束时，您还可以将您的工作记录与“表扬”结果一起登记为您的工作历史。 将传统以“指责”为中心的沟通转变为以“表扬”为中心的沟通，工作场所将变得更加活跃，引发自发的安全行动。

免责声明及风险提示: