南明离火
移动应用检测平台

ANDROID 静态分析报告

Eze • v5.0

分析日期: 2025-07-05 17:28:24

应用概览

文件名称:	Eze v5.0.apk
文件大小:	37.04MB
应用名称:	Eze
软件包名:	com.ezesoft.mobile
主活动:	com.ezesoft.mobile.MainActivity
版本号:	5.0
最小SDK:	26
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:	2/432
杀软检测:	经检测，该文件安全
MD5:	5a6c0442143336c7fec67e8944c19401
SHA1:	b496f5c7ebfa60378b6fa17a8b0a57c2ff7a3307
SHA256:	2052527e8a8b223c0524a55a9e6fd01ca412c3a46814b1c38a967c6346c51a87

分析结果严重性分布

高危	中危	信息	安全	关注
3	11	4	2	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 1个
Service组件：7个，其中export的有： 1个
Receiver组件：2个，其中export的有： 0个
Provider组件：6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: 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: 2020-10-28 09:27:42+00:00
有效期至: 2050-10-28 09:27:42+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x8124aad97acd7805cf35b96d7de3a74dee9784fe
哈希算法: sha256
证书MD5: ba9c13178c3ae95b2906cb909a117eae
证书SHA1: 1f9f45df0b3ffe05aedf4577f9ad82c19902be5c
证书SHA256: 28fbb67e642a4ef8da3243c619c60ba597ca8fb88eccd47b44ebb79328bbe4f3
证书SHA512:
5495ce730e46e6e981f964de6f025b1ad86d8d707594f485b20352201a3753b6d59d591763e962e2d52fb373a9e3764881c8d69cee7896767e0b63fa3f299fa7

公钥算法: rsa
密钥长度: 4096
指纹: d017e82504e8d02d7764378955bf4bab3bc2473d9e3872b73a8cb44fc1216151
共检测到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	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.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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。
com.ezesoft.mobile.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.ezesoft.mobile.MainActivity	Schemes: com.ezesoft.mobile://, Hosts: callback,

网络通信安全风险分析

高危: **2** | 警告: **1** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	警告	基本配置配置为信任系统证书。
2	*	高危	基本配置配置为信任用户安装的证书。
3	ocsp.usertrust.com ocsp.sectigo.com ezesoft.net 127.0.0.1 10.0.0.1 10.0.1.1 10.0.2.2 localhost	高危	域配置不安全地配置为允许明文流量到达范围内的这些域。

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: **2** | 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=@xml/network_security_config]	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	Activity (androidx.biometric.DeviceCredentialHandlerActivity) 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。
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。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	此应用程序可能具有Root检测功能	警告	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
3	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
4	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
5	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

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	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
8	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
9	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
10	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
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

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
00013	读取文件并将其放入流中	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
00036	从 res/raw 目录获取资源文件	反射	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

00126	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
00188	获取短信地址	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
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
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
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
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
00043	计算WiFi信号强度	信息收集 WiFi	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

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	1/30	android.permission.WAKE_LOCK
其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
docs.swmansion.com	安全	否	**IP地址:** 172.67.142.188 **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
eze-mobile.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
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

URL 链接安全分析

URL信息	源码文件

• https://docs.amplify.aws/lib/datastore/data-access/q/platform/js • https://git.io/JUIaE • http://s3.amazonaws.com/doc/2006-03-01 • http://johannburkard.de/blog/programming/javascript/highlight-javascript-text-higlighting-jquery-plugin.html • https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting • https://docs.amplify.aws/lib/troubleshooting/upgrading/q/platform/js • http://bxslider.com • http://css3pie.com • https://docs.amplify.aws/lib/datastore/advanced-workflows/q/platform/js • http://www.madcapsoftware.com • http://www.ezesoft.com • https://apps.apple.com/in/app/eze-for-iphone/id1528044898 • https://github.com/aws-amplify/amplify-js/issuescrollbarchart-box-outlinebuttonSelectedItemObjectsChangetAnimationDurationSMPTEnsure • http://www.staff.science.uu.nl • http://www.ummulqura.org.sa/index.aspx • http://www.madcapsoftware.com/Schemas/MadCap.xsd • http://adlnet.gov/expapi/activities/assessment • http://bxcreative.com • http://momentjs.com/guides • http://johannburkard.de • http://www.quirksmode.org/bugreports/archives/2006/01/Explorer_z_index_bug.html • https://redux-toolkit.js.org/Errors?code • https://www.madcapsoftware.com • http://invertase.link/ios • https://commonmark.org • https://play.google.com/store/apps/details?id=com.ezesoft.mobile • http://fb.me/use-check-prop-typesVersionsisIterateeCalling • https://docs.swmansion.com/react-native-reanimated/docs/fundamentals/glossary • https://a.co/48dbdYzoomToRect • https://bit.ly/3cXEKWfirehose.ap-southeast-1.amazonaws.com.amazonaws.firehose • http://github.com/jrburke/requirejs • https://bit.ly/3cXEKWfirehose.ap-south-1.amazonaws.com.amazonaws.firehose • http://foundation.zurb.com • http://invertase.link/android • http://ny4tcg01.ezesoft.net/stats • https://redux.js.org/Errors?code • http://www.zurb.com • https://aws-amplify.github.io/docs/js/authentication • http://fb.me/use-check-prop-types-control-rodent • http://mths.be/placeholder • http://stevenwanderski.com • http://css3pie.com/documentation/known-issues • https://github.com/requirejs/requirejs/blob/master/LICENSE	自研引擎-A
• https://shopify.github.io/flash-list/docs/usage#cellrenderercomponent	com/shopify/reactnative/flash_list/AutoLayoutView.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://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://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
• https://eze-mobile.firebaseio.com	自研引擎-S

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://eze-mobile.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/828521447677/namespaces/firebase:fetch?key=AIzaSyAeIoG_iqcHGjPcnTRMuxemRsomrgkt3fM ） 已禁用。响应内容如下所示： 响应码是 403

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。
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。

第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
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
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://eze-mobile.firebaseio.com"
"google_api_key" : "AIzaSyAeToG_iqcHGjPcnTRNuxemRsomrgkt3fM"
"google_app_id" : "1:828521447677:android:3aa827137dd39be2527e94"
"google_crash_reporting_api_key" : "AIzaSyAeToG_iqcHGjPcnTRNuxemRsomrgkt3fM"

Google Play 应用市场信息

标题: Eze for Android

评分: 0 **安装:** 500+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.ezesoft.mobile

开发者信息: Eze Software, Eze+Software, None, https://www.ezesoft.com/, ezemobileappadmin@ezesoft.com,

发布日期: 2020年11月5日 **隐私政策:** Privacy link

关于此应用:

介绍 全新 Eze 移动体验已登陆您的手机和平板电脑！下一代 SS&C Eze 应用程序由 Eze Eclipse 和 Eze OMS 提供支持，通过简单易用的界面提供对 Eze 应用程序的安全访问。 无论您是交易者还是投资组合经理，SS&C Eze 应用程序都可以帮助您管理您的投资组合并关注绩效，以便您可以在时机成熟时更快地采取行动。 OMS 的 Eze 应用程序 安全快速的登录 • 从登录屏幕上的产品下拉列表中选择您的产品(Eze OMS)。 • 使用开放 ID 身份验证登录 • 使用生物识别技术解锁应用程序 快速查看投资组合信息和分析 • 查看您的投资组合的高级摘要和详细视图，并快速了解您在组级别/聚合级别的投资组合绩效。 • PL(V)/PLBP、风险敞口、MarketVal/Gross 等指标触手可及，并且能够在投资组合级别添加市场价值、货币、港口基础货币等字段。 • 根据您的需要定制数据点。 • 按行业、部门等汇总投资组合！ 您的应用程序，您的配置 • 配置按位置（托管人）或净头寸或策略划分的头寸 • 从头寸状态列表中进行选择，例如建议、发布到市场、已收到填充、最终确定、已确认和已结算。 • 编辑“分析”屏幕中的列。 交易画面 • 您可以随时随地查看交易详情。此外，市场数据集成已上线。 设置屏幕 • 您可以配置默认投资组合设置和交易刷卡选项，以便在取消订单或从主页中删除卡之前快速执行交易或确认。 • 在深色和浅色模式之间切换。 适用于 Eclipse 的 Eze 应用程序 安全快速的登录 • 从登录屏幕上的产品下拉列表中选择您的产品(Eze Eclipse)。 • 使用开放 ID 身份验证登录 • 使用生物识别技术解锁应用程序 快速查看投资组合信息 • 查看实时盘中投资组合的摘要视图并快速了解您的表现。 • 已实现PL(V)/PLBP、未实现PL(V)/PLBP等指标触手可及，并且能够添加市场价值、货币、港口基础货币等字段。 随时随地分析 • 查看包含各种数据点的投资组合的高级摘要 • 根据您的需求自定义数据点 • 按行业、部门等汇总投资组合！ 您的应用程序，您的配置 • 配置按位置（托管人）或净头寸或策略划分的头寸 • 从头寸状态列表中进行选择，例如建议、发布到市场、已收到填充、最终确定、已确认和已结算。 • 编辑分析详细信息屏幕中的列。 交易（贸易记事簿、订单管理和路线管理） • 从 Trade Blotter 创建订单，过滤订单状态和操作过滤订单 • 在交易记事本上查看订单的创建、填写状态和订单进度。 • 根据代码和日期对订单进行排序 • 从交易记事簿和订单详细信息屏幕添加、编辑、取消全部和取消选定订单 • 从订单详细信息和路线详细信息屏幕添加、编辑和取消路线 • 创建交易时添加主安全文件中不存在的新交易品种 设置屏幕 • 您可以配置交易刷卡选项和账户设置，以便在取消订单或从主页中删除卡之前快速执行交易或确认。 • 在深色和浅色模式之间切换。 确保您的数据安全 • SS&C Eze 维持强大的安全框架，并通过了 ISO 27001 认证，包括云安全和云隐私的 ISO 27017 和 27018。 注意：您的组织必须授权访问 SS&C Eze 移动应用程序。您只能根据您的角色访问您的组织已启用的移动功能（并非所有移动功能都可供您使用）。并非所有 SS&C Eze 功能均可在移动设备上使用。

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。