南明离火
移动应用检测平台

ANDROID 静态分析报告

TezFinance - v1.1.1

分析日期: 2025-08-04 10:53:36

应用概览

文件名称:	111.apk
文件大小:	29.47MB
应用名称:	TezFinance
软件包名:	com.finance.tez
主活动:	com.finance.tez.pages.FirstActivity
版本号:	1.1.1
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	53/100 (中风险)
跟踪器检测:	6/432
杀软检测:	6 个杀毒软件报毒
MD5:	352ba9e0c86735966c28ae1dc372a160
SHA1:	1f85b81e46e783fddb41ec28fab4bf718a205577
SHA256:	84ea03972fdd58a478e29c8840d32f192c286f8ac8f6b7cf837fc697dd40889f

分析结果严重性分布

高危	中危	信息	安全	关注
1	25	1	2	0

四大组件导出状态统计

Activity组件：18个，其中export的有： 13个
Service组件：1个，其中export的有： 1个
Receiver组件：6个，其中export的有： 2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: False
v4 签名: False
主题: CN=teztez
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-18 10:26:02+00:00
有效期至: 2050-02-12 10:26:02+00:00
发行人: CN=teztez
序列号: 0x1
哈希算法: sha256
证书MD5: cef8466f014537a7e47fb995b6803c88
证书SHA1: 16d57d7d658cece1d89fd996c848d56177ff289d
证书SHA256: 49622965ded91904556f843700dc0d88cb2f6cb4e005e4f40be1911ee30b4eaf
证书SHA512:
10ed84ded647de4bae8856f1ab680fb1d5f4f2fc4c30872ba1b8c3c7c054d8ce17e4125c1e00cc9ea0ed7780b4e39240bfd0a82a1aa443bdd012de68d9a078fc

公钥算法: rsa
密钥长度: 2048
指纹: 89fb4bd4dda3616c1eda06fc9d99ca92387a3cfeb6eaea4f55b5996a1797d443
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.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.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
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_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.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.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.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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
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.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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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.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.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。
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.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
com.finance.tez.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.finance.tez.pages.DeepLinkActivity	Schemes: tezfinance://, Hosts: deep, Path Prefixes: /data,
com.facebook.CustomTabActivity	Schemes: @7F10007A://, fbconnect://, Hosts: cct.com.finance.tez,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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: **17** | 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=@7F130004]	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.finance.tez.pages.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 (com.finance.tez.pages.PermissionActivity) 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。
5	Activity (com.finance.tez.pages.LoginActivity) 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。
6	Activity (com.finance.tez.pages.BindPhoneAfterAuthActivity) 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	Activity (com.finance.tez.pages.MajorActivity) 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。
8	Activity (com.finance.tez.pages.WebActivity) 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。

9	Activity (com.finance.tez.xcamera.AcquireIdCardActivity) 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。
10	Activity (com.finance.tez.xcamera.SelfieActivity) 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。
11	Activity (com.facebook.CustomTabActivity) 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。
12	Activity (com.izilab.livenesss.api.LivenessActivity) 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。
13	Activity (com.izilab.livenesss.api.UserGuideActivity) 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。
14	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。
15	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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。
16	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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。
17	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。

18	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: **0** | 警告: **6** | 信息: **1** | 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	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
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	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
5	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
6	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

7	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
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
9	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

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/libsurface_util_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。	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

应用行为分析

编号	行为	标签	文件
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
00036	从 res/raw 目录获取资源文件	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
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
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
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
00003	将压缩后的位图数据放入JSON对象中	相机	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
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

00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	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
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
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
00035	查询已安装的包列表	反射	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
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00064	监控来电状态	控制	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00139	获取当前WiFi id	信息收集 WiFi	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
00083	查询IMEI号	信息收集 电话服务	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
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
00038	查询电话号码	信息收集	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

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.READ_PHONE_STATE android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.READ_CONTACTS android.permission.READ_CALL_LOG android.permission.READ_CALENDAR android.permission.REQUEST_INSTALL_PACKAGES android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH 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
server.tezslz8fin.xyz	安全	否	**IP地址:** 3.6.217.253 **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
server.tezfinance.net	安全	否	No Geolocation information available.
tf.tezfinance.co	安全	否	**IP地址:** 15.207.228.56 **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

URL 链接安全分析

URL信息	源码文件
• https://server.tezslz8fin.xyz/sikredit-point/sikredit/point-data	com/finance/tez/lyx/MdyCore.java

• https://tf.tezfinance.co/about.html • https://tf.tezfinance.co/privacy.html • https://tf.tezfinance.co/terms.html	com/finance/tez/tools/IUrlsKt.java
• https://play.google.com/store/apps/details?id=	com/finance/tez/tools/AppStore.java
• https://server.tezslz8fin.xyz/sikredit-api/	com/finance/tez/net/ServerClient.java
• https://server.tezfinance.net	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已启用	警告	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/[illegible]16034813/namespaces/firebase:fetch?key=AIzaSyA_HeutuENUJ[illegible]7MHG1tXiUyyLHKL27Et5s ）已启用。请确保这些配置不包含敏感信息。响应内容如下所示：
		
		{
		"entries": {
		"remote_h5": "home.tezfinance.co",
		"remote_host": "server.tezril85[illegible]kr.xyz",
		"remote_html": "tf.tezfinance.co",
		"switch_remote_h5": "false"
		},
		"state": "UPDATE",
		"templateVersion": "1"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
ML Kit	Google	ML Kit 将功能强大且易于使用的软件包将 Google 的机器学习专业知识带给移动开发人员。使用经过优化可在设备上运行的解决方案，让您的 iOS 和 Android 应用程序更具吸引力、个性化和有用。
Jetpack CameraX	Google	CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地向应用添加相机功能。该库提供了很多兼容性修复程序和解决方法，有助于在众多设备上打造一致的开发者体验。
Google Sign-In	Google	提供使用 Google 登录的 API。
Google Play Services	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。

本报告由南明离火移动安全分析平台生成

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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
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"
"password" : "Password"
"google_api_key" : "AIzaSyA_HeutuENUgc7MHG1tXiUyyLHKL27Et5s"
"firebase_web_client_id" : "1:750016034813-b05fgg5n7756jqlcgh4efbo8jp978bhc.apps.googleusercontent.com"
"google_app_id" : "1:750016034813:android:e8f8e03d5d789e71e33b94"
"facebook_client_token" : "c03509e6e1587d84b100de258752dd1c"
"facebook_app_id" : "1086771069088701"
"google_crash_reporting_api_key" : "AIzaSyA_HeutuENUgc7MHG1tXiUyyLHKL27Et5s"

8a3c4b262d721acd49a4bf97d5213199c86fa2b9
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
cc2751449a350f668590264ed76692694a80308a
9b8f518b086098de3d77736f9458a3d2f6f95a37
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
c56fb7d591ba6704df047fd98f535372fea00211

免责声明及风险提示:

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。