南明离火
移动应用检测平台

ANDROID 静态分析报告

Equitas • v1.0.1

分析日期: 2025-03-11 13:39:02

应用概览

文件名称:	Equitas v1.0.1.apk
文件大小:	18.13MB
应用名称:	Equitas
软件包名:	com.equitas.mobile
主活动:	com.equitas.mobile.MainActivity
版本号:	1.0.1
最小SDK:	22
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:	59/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	df1c757ce3b2a2934926ac806dfd3663
SHA1:	b1028327183d2683ac80112d9e1d1ae218e1f582
SHA256:	2ef5c04cdab623b36bc413e9804eaa52c2dac3421d3e7f5407cae519dc5c5a36

分析结果严重性

高危	中危	信息	安全	关注
1	7	2	2	0

四大组件信息

Activity组件：3个，其中export的有：1个
Service组件：6个，其中export的有：0个
Receiver组件：2个，其中export的有：1个
Provider组件：3个，其中export的有：0个

证书信息

二进制文件已签名
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: 2024-07-21 23:44:54+00:00
有效期至: 2054-07-21 23:44:54+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xa5998676f04c120f7d4e771dff34bdec371f6636
哈希算法: sha256
证书MD5: d5430e44cfb5375f582841b2a5aa8ba6
证书SHA1: 155a7b2bcd7be5cad669fcfb89dec35187cb6007
证书SHA256: 985f00b3da1f85140974daf3c50d12bc3a342e4f1367c21f8181ce275da78caa
证书SHA512:
b884f2ea14dc56de5021872b2cc4d27a3a3588c0a418f584a189a1fb2a098f6d506d4130799305503598f80ae444fcaba52332e5[illegible]c15166360d4c393b

公钥算法: rsa
密钥长度: 4096
指纹: 96f09c59683287ec70cd883b90023019cdc6362b1023e7f66233f77a39f413dc
找到 1 个唯一证书

应用权限

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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
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.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.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
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.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.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。

可浏览的Activity组件

ACTIVITY	INTENT
com.equitas.mobile.MainActivity	Schemes: https://, Hosts: equitas.site,

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **1** | 警告: **1** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	App 链接 assetlinks.json 文件未找到 [android:name=com.equitas.mobile.MainActivity] [android:host=https://equitas.site]	高危	App Link 资产验证 URL （https://equitas.site/.well-known/assetlinks.json）未找到或配置不正确。（状态代码：None）。应用程序链接允许用户从 Web URL 发送邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确，则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击，泄露 URI 中的敏感数据，例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android：autoVerify="true"] 启用验证来验证 App Link 网域。
2	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

安全漏洞检测

高危: **0** | 警告: **5** | 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
3	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
4	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
5	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
6	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
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

行为分析

编号	行为	标签	文件
00192	获取短信收件箱中的消息	短信	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
00028	从assets目录中读取文件	文件	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
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
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

00091	从广播中检索数据	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
00036	从 res/raw 目录获取资源文件	反射	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
00012	读取数据并放入缓冲流	文件	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
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
00007	Use absolute path of directory for the output media file path	文件	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
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
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	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
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	升级会员：解锁高级权限
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.RECEIVE_BOOT_COMPLETED android.permission.VIBRATE android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE

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。

域名检测

域名	状态	中国境内	位置信息
capacitorjs.com	安全	否	**IP地址:** 172.67.203.214 **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
www.zetetic.net	安全	否	**IP地址:** 18.154.206.82 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图

URL链接分析

URL信息	源码文件

• https://www.googletagmanager.com/gtag/js • https://capacitorjs.com/ • https://www.google.com/recaptcha/enterprise.js?render= • https://stackoverflow.com/q/56496296/110915 • https://stenciljs.com/docs/properties • http://momentjs.com/guides/ • https://github.com/kripken/emscripten/issues/5820 • https://equitas.site/automatic-assistant/ • https://ionic.io • https://firebase.google.com/docs/web/environments-js-sdk • https://firebase.google.com/pricing/. • https://stenciljs.com/docs/templating-jsx • https://stackoverflow.com/a/57382543 • https://stuk.github.io/jszip/documentation/howto/read_zip.html • https://angular.io/license • https://mozilla.github.io/localForage/ • https://g.co/ng/security • https://stackoverflow.com/questions/29249132/wkwebview-complex-communication-between-javascript-native-code/49474323 • https://api.equitas.site/ • https://apis.google.com/js/api.js • http://drifty.com/ • https://equitas.site/mentions-legales-et-conditions-dutilisation/ • https://securetoken.google.com/ • https://www.google.com/recaptcha/api.js	自研引擎-A
• https://capacitorjs.com/docs/apis/splash-screen#hiding-the-splash-screen	com/capacitorjs/plugins/splashscreen/SplashScreen.java
• https://github.com/sqlcipher/android-database-sqlcipher • https://www.zetetic.net/sqlcipher/ • https://www.zetetic.net/sqlcipher/license/	自研引擎-S

FIREBASE数据库分析

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/834539345585/namespaces/firebase:fetch?key=AIzaSyApXBTZT2vD8ZBlrkLD9HfmXFX7SopbeJk） 已禁用。响应内容如下所示:
		
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

SDK名称	开发者	描述信息
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 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。

密钥凭证

可能的密钥
"google_api_key" : "AIzaSyApXBTZT2vD8ZBlrkLD9HfmXFX7SopbeJk"
"google_app_id" : "1:834539345585:android:05f161fc81340516ac7490"
"google_crash_reporting_api_key" : "AIzaSyApXBTZT2vD8ZBlrkLD9HfmXFX7SopbeJk"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"

GooglePlay应用信息

标题: Equitas

评分: 4.2 **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 教育 **Play Store URL:** com.equitas.mobile

开发者信息: Equitas Soft, Equitas+Soft, None, https://equitas.site, contact@equitas.site,

发布日期: 2024年7月27日 **隐私政策:** Privacy link

关于此应用:

Equitas 是一个由非政府组织合作伙伴组成的欧洲网络，其目的是为仇视伊斯兰教的受害者提供援助，并更好地了解欧洲的仇视伊斯兰教现象。 在此应用程序中，您可以 - 举报仇视伊斯兰教的行为，该行为将由法律团队处理 - 了解您的权利 - 了解欧洲伊斯兰恐惧症的最新动态

免责声明及风险提示: