南明离火
移动应用检测平台

ANDROID 静态分析报告

Vesuvius • v228

本报告由南明离火移动安全分析平台生成

分析日期: 2025-08-02 20:14:15

应用概览

文件名称:	Vesuvius v228.apk
文件大小:	30.23MB
应用名称:	Vesuvius
软件包名:	com.volcanex.vesuvius
主活动:	.main
版本号:	228
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:	53/100 (中风险)
跟踪器检测:	3/432
杀软检测:	经检测，该文件安全
MD5:	b470aab2006b22db5b72cdb40d9a2c1b
SHA1:	cf8f8adc7bddea77f581d2054e51a3ba4489eb81
SHA256:	3b12e636e96cb8b1759adee1cb4dc36add78047e79bd606e8de14c3735ae2ab

分析结果严重性分布

高危	中危	信息	安全	关注
1	20	1	2	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 0个
Service组件：9个，其中export的有： 3个
Receiver组件：12个，其中export的有： 9个

Provider组件：4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: 2022-06-26 03:51:30+00:00
有效期至: 2052-06-26 03:51:30+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xb828f54a930bde2b59a773087dd6a4c19b1ac0cb
哈希算法: sha256
证书MD5: 0e52471ede9cc0a9c112ec2c63af1480
证书SHA1: 5c48e68b61ceda165d91d984d4ffae25319b1011
证书SHA256: 0e82a99abc16660624d74ad182a2cdfeb3d43017a401b09269af109dd40dcb8d
证书SHA512:
32eff3348c0f586f875739712e9623f493ad05fff5f4122608105cb6363da5e87bf456a5041[illegible]dd18[illegible]485f045d25869[illegible]f74dd025add3febf3f4d810918c77

公钥算法: rsa
密钥长度: 4096
指纹: 3c77dd9a9857fe2f1750a11f07532bb8e883d6bfd552ddb0cce2c74f8[illegible]37e8
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
com.volcanex.vesuvius.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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.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。
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。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
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.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.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。

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.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。
com.volcanex.vesuvius.permission.MAPS_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
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（推送意外播放，锁屏播放）
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.WAKE_LOCK	危险	防止手机休眠	允许应用程序阻止手机休眠，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.volcanex.vesuvius.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.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: **1** | 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	应用已配置网络安全策略 [android:networkSecurityConfig=@7F120004]	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。
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	Service (com.google.firebase.iid.FirebaseInstanceIdService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
5	Service (anywheresoftware.b4a.objects.FirebaseNotificationsService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
6	Broadcast Receiver (.firebasemessaging) 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。
7	Broadcast Receiver (.ftpcamvideo) 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。
8	Broadcast Receiver (.eadb) 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。
9	Broadcast Receiver (.location) 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。
10	Broadcast Receiver (.startatbootreceiver) 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。
11	Service (.starter) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。

12	Broadcast Receiver (.starter$starter_BR) 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。
13	Broadcast Receiver (.webcamload) 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。
14	Broadcast Receiver (.httputils2service) 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: **5** | 信息: **1** | 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
3	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
4	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
5	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

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	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
8	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
00013	读取文件并将其放入流中	文件	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
00163	创建新的 Socket 并连接到它	Socket	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
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
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
00204	获取默认铃声	信息收集	升级会员：解锁高级权限

00146	获取网络运营商名称和 IMSI	电话服务 信息收集	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
00193	发送短信	短信	升级会员：解锁高级权限
00117	获取 IMSI 和网络运营商名称	电话服务 信息收集	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
00091	从广播中检索数据	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.gms.permission.AD_ID android.permission.FOREGROUND_SERVICE 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
graemewheller.com	安全	否	**IP**地址: 46.202.172.30 国家: 法国 地区: 法兰西岛 城市: 巴黎 纬度: 48.859077 经度: 2.293486 查看: Google 地图

URL 链接安全分析

URL信息	源码文件
• http://doi.org/10.1029/JB088iB08p06357 • http://doi.org/10.1007/s00445-004-0348-8C • http://doi.org/10.1029/2006EO400001 • http://doi.org/10.1017/S0016756809990495P • http://doi.org/10.1098/rstl.1768.0001V • http://doi.or • http://doi.org/10.1007/s00445-005-0414-x • http://doi.org/10.1007/s00445-004-0348-8 • http://doi.org/10.1016/j.jvolgeores.2008.06.009 • http://doi.org/10.3406/quate.1998.2104 • http://doi.org/10.2307/504292 • http://doi.org/10.1016/j.quascirev.2014.10.028 • http://doi.org/10.1007/s007100170011 • http://doi.org/10.1007/s00445-004-0348-8B • http://doi.org/10.1016/j.jvolgeores.2010.11.0218 • https://doi.org/10.1016/j.jvolgeores.2021.107245pa • http://doi.org/10.1016/j.jvolgeores.2007.12.004nY • http://doi.org/10.1016/j.jvolgeores.2007.08.001 • http://doi.org/10.1038/35071167 • http://doi.org/10.1016/j.quascirev.2009.06.009 • https://www.facebook.com/vesuviusvolcanopedia • http://doi.org/10.1093/petrology/egl081 • http://doi.org/10.1007/s11069-016-2182-7 • http://www.ov.ingv.it/ov/it/bollettini/275.htmlp • http://doi.org/10.1016/j.quascirev.2014.10.028B • http://doi.org/10.1007/s00445-010-0379-2Q • http://www.protezionecivile.gov.it/attivita-rischi/rischio-vulcanico/vulcani-italia/flegrei/pian o-nazionale-di-protezione-civileq • http://doi.org/10.1016/0377-0273 • http://doi.org/10.3931/e-rara-23388AJ • http://doi.org/10.1007/s00445-011-0454-3V • https://doi.org/10.1016/j.earscirev.2018.11.007J • http://www.protezionecivile.gov.it/attivita-rischi/rischio-vulcanico/vulcani-italia/flegrei/pian o-nazionale-di-protezione-civilex • http://doi.org/10.1016/S0377-0273 • http://doi.org/10.1029/94EO00738 • http://doi.org/10.1016/j.jvolgeores.2006.08.006 • https://doi.org/10.1007/s00445-010-0379-2 • https://archive.org/details/storiadellincen00real • https://doi.org/10.1016/S0377-0273 • http://gallica.bnf.fr/ark • http://doi.org/10.1130/0016-7606 • http://doi.org/10.1016/j.jvolgeores.2007.10.007l • http://www.ov.ingv.it/ov/it/bollettini/275.html • http://doi.org/10.1073/pnas.0506691103	自研引擎-A
• http://91.108.112.177:52893/vclast • http://91.108.112.177:52892/fvs	com/volcanex/vesuvius/b4xmainpage.java
• http://91.108.112.177:52893	com/volcanex/vesuvius/eqdb.java
• http://91.108.112.177:52894/fcm	com/volcanex/vesuvius/eqmessaging.java
• https://invalid-url/	com/volcanex/vesuvius/httpjob.java

• https://graemewheller.com/app-privacy/	com/volcanex/vesuvius/pagesettings.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/470776339167/namespaces/firebase:fetch?key=AIzaSyC7WAwybbpHD9yo4WRc9tmiqjevsYAyXCE ） 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
Jetpack Test	Google	在 Android 中进行测试。
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建模块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建模块。
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。
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 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。

邮箱地址敏感信息提取

EMAIL	源码文件
graemewheller@gmail.com	com/volcanex/vesuvius/pagesettings.java

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
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
凭证信息=> "com.google.android.geo.API_KEY" : "AIzaSyAhlwygFco1XypvdvG8wV9YkxkWs8PAhw"
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-7097999391510745~9780826090"
"google_api_key" : "AIzaSyC7WAwybbpHD9yo4WRc9tmiqjevsXAxXCE"
"google_app_id" : "1:470776339167:android:4f04b14fa4c5ec0[illegible]e75a"
"google_crash_reporting_api_key" : "AIzaSyC7WAwybbpHD9yo4WRc9tmiqjevsXAxXCE"
6E51BE88E792DC8C7FA674C6C7448B38

Google Play 应用市场信息

标题: Vesuvius Volcano

评分: 4.076923 **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 外出旅行与本地生活 **Play Store URL:** com.volcanex.vesuvius

开发者信息: Graeme Wheller, Graeme+Wheller, None, https://graemewheller.com, graemewheller@gmail.com,

发布日期: 2022年7月5日 **隐私政策:** Privacy Policy

关于此应用:

该应用程序由独立的火山学家开发，可让您近乎实时地跟踪意大利坎帕尼亚维苏威火山的火山地震。 自 1944 年上次爆发以来，维苏威火山已成为主要的旅游目的地，每年约有 300 万游客，另有 300 万人居住在其两侧。它的活动受到非常密切的监控，这个应用程序提供了一个方便的视图，可以方便地查看用于喷发风险评估的地震数据的主要部分。 地震数据由意大利国家地球物理与火山研究所（INGV-OV）的维苏威火山天文台获得。该应用程序会定期下载这些数据并创建时间序列图，显示地震频率、震级和深度的趋势。如果您在该地区，震中也会与官方危险区域的地图和您所在的位置一起绘制在交互式地图上。该应用程序旨在轻松访问重要的火山学数据，这将吸引想要监测可能影响维苏威火山喷发风险的任何重大变化的居民和游客。 对于附近的居民，该应用程序将快速提供您可能感觉到的任何地震的详细信息。它还提供地震仪功能，当您的手机接通电源时，该功能将自动运行。这可以显示您晚上睡觉时您的房子是否受到任何地震的影响。它还可以显示维苏威火山周围的所有位置，如 500 x 500 m 正方形，应用地震仪检测到地震的地方。 （*该应用程序与 INGV-OV 无关，也不受其支持。有关维苏威火山风险的官方信息，请访问 https://www.ov.ingv.it）。

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。