南明离火
移动应用检测平台

ANDROID 静态分析报告

.Geometry Dash

分析日期: 2024-08-02 11:03:08

应用概览

文件名称:	Geometrydash.apk
文件大小:	2.11MB
应用名称:	.Geometry Dash
软件包名:	com.dgn.kgu
主活动:	com.boytaoto.vippro.home.MainActivity
版本号:	
最小SDK:	22
目标SDK:	33
加固信息:	未加壳
应用程序安全分数:	54/100 (中风险)
杀软检测:	23 个杀毒软件报毒
MD5:	0e422172b8c7c7398b5382a60c485c44
SHA1:	2a47b6c84acbff0351cf98cd55288aacc8dc9c4e
SHA256:	7521a09ced6aab36ee75e4c5f0db75f663616015246091fbc055f86c709dcf27

分析结果严重性分布

高危	中危	信息	安全	关注
3	8	2	3	2

四大组件导出状态统计

Activity组件：2个，其中export的有：1个
Service组件：7个，其中export的有：1个
Receiver组件：8个，其中export的有：1个
Provider组件：1个，其中export的有：0个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: True

本报告由南明离火移动安全分析平台生成

v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2014-11-06 19:07:40+00:00
有效期至: 2042-03-24 19:07:40+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x970f983909aa8949
哈希算法: sha1
证书MD5: db18d311f507489595b5a450bb2dc495
证书SHA1: 14a33cebe3e8667b409ef8142a9d56259ec8328e
证书SHA256: 8ad127abae8285b582ea36745f220ab8fe397ffb3b068df19ca22d122c7b3b86
证书SHA512:
72ea616d1d4abd371a4666b9b1300230766c0ec47b52af410e64a60d6067be9c8f37bafb2f54abca90d82cc1983e372ba2e2458f80e29facc8f8167d842deae2

公钥算法: rsa
密钥长度: 2048
指纹: 763d397255e11ff2bf6f79c6971a1ff9b3796d030008ffca2fe3dc495dacf6b4
找到 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.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android P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.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.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。

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	应用程序已使用代码签名证书进行签名

Manifest 配置安全分析

本报告由南明离火移动安全分析平台生成

高危: **0** | 警告: **5** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.1-5.1.1, [minSdk=22]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据，它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Activity (com.boytaoto.vippro.home.SearchActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service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。
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。

代码安全漏洞检测

高危: **2** | 警告: **3** | 信息: **2** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序使用SQLite数据库执行原始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
2	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

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	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
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	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
8	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
9	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	4/30	android.permission.SEND_SMS android.permission.SYSTEM_ALERT_WINDOW android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	3/46	android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NETWORK_STATE

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
vilandsoft.com	病毒 **URL:** vilandsoft.com **IP:** N/A **Description:** Maltrail 标记的恶意域	是	**IP地址:** 47.242.162.24 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.15769 **查看:** 高德地图
onesignal.modobomco.com	安全	否	**IP地址:** 139.162.35.31 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850381 **查看:** Google 地图
www.google.co.th	安全	否	**IP地址:** 32.250.42.157 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
www.duckduckgo.com	安全	否	**IP地址:** 209.73.190.11 **国家:** 美利坚合众国 **地区:** 华盛顿 **城市:** 昆西 **纬度:** 47.234463 **经度:** -119.852577 **查看:** Google 地图
www.bing.com	安全	否	**IP地址:** 23.206.229.209 **国家:** 美利坚合众国 **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
www.yahoo.com	安全	否	**IP地址:** 209.73.190.11 **国家:** 美利坚合众国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.731323 **经度:** -73.990089 **查看:** Google 地图

sdk1.vilandsoft.com	安全	是	**IP地址:** 47.242.162.24 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
onesignal5.modobomco.com	安全	否	**IP地址:** 47.242.162.24 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
apkafe.com	安全	否	**IP地址:** 104.21.21.76 **国家:** 美利坚合众国 **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

URL 链接安全分析

URL信息	源码文件
• https://www.google.com	com/telpoo/frame/net/BaseNetData.java
• http://onesignal5.modobomco.com/add-player-id-lock • http://onesignal5.modobomco.com/add-onesignal-sms-info • http://onesignal5.modobomco.com/add-player-id • http://onesignal5.modobomco.com/count-app • http://onesignal5.modobomco.com/push-system • http://onesignal5.modobomco.com/get-push-system-config • http://onesignal5.modobomco.com/store-log-behavior • https://onesignal.modobomco.com/api/keywords-info • http://onesignal5.modobomco.com/add-user-active-push-system • http://onesignal5.modobomco.com/apkload-web • http://onesignal5.modobomco.com/update-log-behavior	com/boytaoto/vippro/net/MyUrl.java
• https://apkafe.com/how-to-download-geometry-dash-apk-for-latest-android-phones-2022/	com/boytaoto/vippro/BuildConfig.java
• https://www.yahoo.com • https://www.google.co.th/ • https://www.bing.com/ • https://www.google.com/search?q= • https://www.duckduckgo.com/ • https://apkafe.com/ • https://apkafe.com • https://www.google.co.th/search?q=	com/boytaoto/vippro/spweb/WebObjSpr.java
• https://apkafe.com	com/boytaoto/vippro/home/SearchActivity.java
• https://www.google.com	com/boytaoto/vippro/net/MyData.java
• http://vilandsoft.com/api/mobile/getsetting.php?app_id=	com/telpoo/frame/utils/Cons.java

• https://play.google.com/store/apps/details?id=	com/telpoo/frame/utils/IntentSupport.java
• http://sdk1.vilandsoft.com/check-update?	com/telpoo/frame/fwtask/FrameworkTask.java
• https://www.bing.com/ • http://onesignal5.modobomco.com/add-onesignal-sms-info • http://onesignal5.modobomco.com/get-push-system-config • https://apkafe.com/ • https://www.google.com/search?q= • https://www.google.com • http://onesignal5.modobomco.com/update-log-behavior • http://sdk1.vilandsoft.com/check-update? • http://vilandsoft.com/api/mobile/getsetting.php?app_id= • http://onesignal5.modobomco.com/add-user-active-push-system • http://onesignal5.modobomco.com/apk/load-web • https://www.yahoo.com/ • http://onesignal5.modobomco.com/add-player-id-lock • https://www.duckduckgo.com/ • http://onesignal5.modobomco.com/add-player-id • http://onesignal5.modobomco.com/store-log-behavior • https://play.google.com/store/apps/details?id= • https://apkafe.com • https://www.google.co.th/ • http://onesignal5.modobomco.com/count-app • http://onesignal5.modobomco.com/push-system • https://onesignal.modobomco.com/api/keywords-info • https://www.google.co.th/search?q= • https://apkafe.com/how-to-download-geometry-dash-apk-for-latest-android-phones-2022/	内研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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 库为提供了一种直接，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。
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。

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。