南明离火
移动应用检测平台

ANDROID 静态分析报告

Chemistry game：V3.0.7

分析日期: 2025-03-11 18:10:52

应用概览

文件名称:	com-misho-chemistry-38-61327394-89abe57fe8d06e2675594fa9d8366360.apk
文件大小:	4.23MB
应用名称:	Chemistry game
软件包名:	com.Misho.Chemistry
主活动:	com.Misho.Chemistry.ui.activities.SplashScreenActivity
版本号:	3.0.7
最小SDK:	16
目标SDK:	30
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	58/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	ac014d52d7ad591fedced13a82cb0cbd
SHA1:	41144509064aac169a8d8b1c3ced29b3cc7e26e0
SHA256:	d611d7ccf9f8c1c45d873757[illegible]d5fd9772d8b1a8953d131a587fc06ea3bf1bd45

分析结果严重性

高危	中危	信息	安全	关注
0	7	2	1	0

四大组件信息

Activity组件：5个，其中export的有： 1个
Service组件：8个，其中export的有： 2个
Receiver组件：3个，其中export的有： 0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: False
v4 签名: False
主题: C=BA, ST=Republika Srpska, L=Milići, CN=Misho M. Petkovic
签名算法: rsassa_pkcs1v15
有效期自: 2014-04-29 22:52:43+00:00
有效期至: 2039-04-23 22:52:43+00:00
发行人: C=BA, ST=Republika Srpska, L=Milići, CN=Misho M. Petkovic
序列号: 0x7f0fe291
哈希算法: sha256
证书MD5: dc0e311be5a26c1f633f9399f75a62da
证书SHA1: c3e6a91c8aafbf50a2be4b5e61611a5a5fabe5dc
证书SHA256: c3c7108ebba7fa3c4d95127dfea3e0c717164ddfd7681ad4e46ff111abfa6294
证书SHA512:
bbf0013fcd65ea8710e0056670295da89d7d82cc17348c693487340631058 4f901f82531591f8b4e4ae2e1d96cc776b9c90e293ddccfbd6574e774e8dd2718d

公钥算法: rsa
密钥长度: 2048
指纹: c702776bcb1eb77663b36d4f3e762e3a6608778792c91853a36e8018d4d07292
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.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.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.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.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。

可浏览的Activity组件

ACTIVITY	INTENT
com.Misho.Chemistry.ui.activities.GameActivity	Schemes: http://, https://, Hosts: 1024game.com/,

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: 0 | 警告: 4 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	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。
2	Activity (com.Misho.Chemistry.ui.activities.GameActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
3	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。
4	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。

安全漏洞检测

高危: 0 | 警告: 1 | 信息: 1 | 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	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

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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE 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。

域名检测

域名	状态	中国境内	位置信息
goo.gl	安全	否	**IP地址:** 142.250.72.174 **国家:** 美国 **地区:** 科罗拉多州 **城市:** 丹佛 **纬度:** 39.739361 **经度:** -104.983597 **查看:** Google 地图
admob-app-id-5994518214.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **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

URL链接分析

URL信息	源码文件
• https://goo.gl/bibqze • https://admob-app-id-5994518214.firebaseio.com • https://play.google.com/store/apps/details?id=com.misho.chemistry • https://goo.gl/kcq9v5	自研引擎-S

FIREBASE数据库分析

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://admob-app-id-5994518214.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/109440260004/namespaces/firebase:fetch?key=AIzaSyAEq8rZ0UV_qvJDPQ8luJfm2gZIOqpe1h8 ） 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 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 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。
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 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。

追踪器

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

密钥凭证

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-6504229951563708~5994518214"
凭证信息=> "com.google.android.gms.games.APP_ID" : "@string/app_id"
"app_id" : "642855799355"
"firebase_database_url" : "https://admob-app-id-5994518214.firebaseio.com"
"google_api_key" : "AIzaSyAEq8rZ0UV_qvJDPQ8luJfm2gZIOqpe1h8"
"google_app_id" : "1:109440260004:android:4fe3cead132749d7"

"google_crash_reporting_api_key" : "AIzaSyAEq8rZ0UV_qvJDPQ8luJfm2gZIOqpe1h8"

GooglePlay应用信息

标题: Chemistry game

评分: 3.940594 **安装:** 100,000+ **价格:** 0 **Android版本支持:** **分类:** 教育 **Play Store URL:** com.Misho.Chemistry

开发者信息: Orange Unit, 4648133023405944811, Kralja Petra 10a 11000 Belgrade, Serbia 75446 Milići, Republic of Serbska viber, whatsup +381653333093, http://2048alphabet.com/chemistry/, misho@misho.in.rs,

发布日期: 2014年5月3日 **隐私政策:** Privacy link

关于此应用:

欢迎来到化学游戏，这是一款令人上瘾的益智游戏，它将测试您的化学知识！加入元素并制作 Na 图块！ H+H->He，He+He->Li 等等 凭借直观的游戏玩法和令人惊叹的图形，化学游戏是任何喜欢化学或只是享受良好拼图挑战的人的完美游戏。无论您是化学专业的学生、科学爱好者，还是只是在寻找一种有趣的方式来打发时间，化学游戏都是适合您的游戏。 但是请注意，此游戏非常容易上瘾，一旦开始玩，您将无法停止！那你还在等什么？现在玩，看看你能在元素周期表上走多远！ 该游戏基于 1024（http://1024game.org） Fork 源代码来自 github https://github.com/mishop/2048-chemistry-android

免责声明及风险提示: