南明离火
移动应用检测平台

ANDROID 静态分析报告

Ice Cream Popsicles Games •
v2.1.0

分析日期: 2024-07-07 15:29:36

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

应用概览

文件名称:	df539275b7db6568cb446bd45effa13018a37b1e8136dd8936ffbc9f216a8b6b.apk
文件大小:	7.8MB
应用名称:	Ice Cream Popsicles Games
软件包名:	com.yskj.icpg.huawei
主活动:	com.fakerandroid.boot.UnityPlayerActivity
版本号:	2.1.0
最小SDK:	19
目标SDK:	29
加固信息:	360加固 加固
应用程序安全分数:	39/100 (高风险)
跟踪器检测:	3/432
杀软检测:	4 个杀毒软件报毒
MD5:	f4ae556badaa6a7e1a9dc5d73181d6bc
SHA1:	71bf2e6747895fdf44aa69a295fb971dcc359fb
SHA256:	df539275b7db6568cb446bd45effa13018a37b1e8136dd8936ffbc9f216a8b6b

分析结果严重性分布

高危	中危	信息	安全	关注
4	15	1	0	0

四大组件导出状态统计

Activity组件：14个，其中export的有： 2个
Service组件：3个，其中export的有： 1个
Receiver组件：0个，其中export的有： 0个
Provider组件：1个，其中export的有： 1个

应用签名证书信息

二进制文件已签名

本报告由南明离火移动安全分析平台生成

v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: CN=xp03 OU=xp03
签名算法: rsassa_pkcs1v15
有效期自: 2022-12-20 03:47:06+00:00
有效期至: 2025-12-19 03:47:06+00:00
发行人: CN=xp03 OU=xp03
序列号: 0x72a2d76f
哈希算法: sha256
证书MD5: b1a0825cb01d7b573b3ece63f6d91624
证书SHA1: 962d2c8336bfa2cba4c158181235a3b38f3c2b95
证书SHA256: 5b4c34f8ce04a0d1c3debf9b88cd42cc8504ffee8c5342f5eaa9b61cdcaae5ed
证书SHA512:
61b5fde7e97aaed2117af0c4abc52c259df7cfd6cb11dc2a19390e9106e605eed8727784062ed90fbc4f2686471cfb4d5a7e09ea02cba7bcd6836ce0f26e8ec9

公钥算法: rsa
密钥长度: 2048
指纹: 502c85aff45a8c8f3e2aa9bc8b733d28a3185d35409319c2944bf66294093f6d
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.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
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.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错略的经纬度信息，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。
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.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。
android.permission.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。
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.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。
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.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.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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.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.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.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.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（推送悬浮播放，锁屏播放）
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。
com.huawei.hwid.permission.gameservice.archive.access.provider	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.huawei.openalliance.ad.activity.PPSLauncherActivity	Schemes: hwpps://, Hosts: com.skj.icpg.huawei,

网络通信安全风险分析

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

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。
2	*	警告	基本配置配置为信任系统证书。

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

高危: **1** | 警告: **6** | 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 4.4-4.4.4, [minSdk=19]	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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
4	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。
5	Activity (com.fakerandroid.boot.UnityPlayerActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
6	Activity (com.jx.go.opsdk.SplashActivity) 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。
7	Service (com.huawei.hms.jos.games.service.GameService) 未被保护。 [android:exported=true]	警告	发现 Service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。
8	Content Provider (com.huawei.hms.jos.games.archive.ArchiveRemoteAccessProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
9	Activity (com.huawei.openalliance.ad.activity.PPSLauncherActivity) 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。

代码安全漏洞检测

高危: **2** | 警告: **6** | 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	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

3	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
4	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
5	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
6	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
7	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
8	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
9	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

敏感权限滥用分析

类型	匹配	权限

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

恶意软件常用权限	8/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.SYSTEM_ALERT_WINDOW android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	8/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.BROADCAST_STICKY android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE

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
duckbillgames.xyz	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://47.104.86.96:8529/handler/getonegameconfig.ashx	cn/egmap/app/ggfz/openSdk/ShowOpenIF.java
• http://47.105.43.84:8000/handler/getonegameconfig.ashx	com/fakerandroid/boot/JXH.java
• https://duckbillgames.xyz/huawei/hwgames/popsiclestack/ • https://duckbillgames.xyz/huawei/hwgame/popsiclestack/	com/fakerandroid/boot/UnityPlayerActivity.java
• https://ip.taobao.com/ipsearch?ipaddr=myip • http://120.78.213.12:8090/testopen/getpinfo • http://handler/getonegameconfig.ashx	cn/egmap/app/ggfz/open/b/a.java
• http://47.104.86.96:8000/handler/getonegameconfig.ashx • http://120.78.213.12:8090/testopen/getpinfo	cn/egmap/app/ggfz/open/aut/c.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
华为帐号服务	Huawei	通过华为帐号开放服务，Android 应用可以方便、安全地实现快速登录授权、读取短信验证码等功能，凭借用户授权凭证，应用可快速访问调用华为提供的公开 API。
HMS Update	Huawei	用于 HMS SDK 引导升级 Huawei Mobile Services(APK)，提供给系统安装器读取升级文件。
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView，极度容易使用以及功能强大的库，提供了Android WebView 一系列的问题解决方案，并且轻量和极度灵活。
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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。

第三方追踪器检测

名称	类别	网址
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=102111081"
63a1459088ccdf4b7ea913fa

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。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成