南明离火
移动应用检测平台

ANDROID 静态分析报告

趣友 • v1.0.0

分析日期: 2025-04-05 14:45:26

应用概览

文件名称:	趣友.apk
文件大小:	19.93MB
应用名称:	趣友
软件包名:	com.dangdanggame.csmj
主活动:	com.dangdanggame.csmj.MainActivity
版本号:	1.0.1
最小SDK:	22
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:	50/100 (中风险)
跟踪器检测:	2/432
杀软检测:	AI评估：安全
MD5:	3fea3b7b08847fe5cdb8a951ab26d096
SHA1:	0639628b5b6c6829db73f213560821572642df9f
SHA256:	c8766e2331a25304c0f5293464397f473a15a45bcfab1645a6968c02ac0252

分析结果严重性分布

高危	中危	信息	安全	关注
0	7	2	0	0

四大组件导出状态统计

Activity组件：4个，其中export的有： 2个
Service组件：0个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0个
Provider组件：0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: False
v4 签名: False
主题: C=, ST=, L=, O=, OU=, CN=chh
签名算法: rsassa_pkcs1v15
有效期自: 2016-04-04 22:45:19+00:00
有效期至: 2116-03-11 22:45:19+00:00
发行人: C=, ST=, L=, O=, OU=, CN=chh
序列号: 0x1f9192c
哈希算法: sha256
证书MD5: 21e21062b7c9d53f1b6ec568beabfd20
证书SHA1: d4f52293d79e26a85a1c255d35ccb3813c4aee20
证书SHA256: 4677ce4c585e76f8f9462c468087768cd96c81ccd21fa9c2dd77fd0d4d81d39b
证书SHA512:
b988aa0ba9fe1d42c374cf5c7a01246919b6225160c2ad02dd537265420e4970075c8885f3bad7b97d2c6c2bbd8ed0ad138c6011a9d3615ef3549ec781e176fd

公钥算法: rsa
密钥长度: 2048
指纹: d410da6393b5e8fbe66f417d3416d901581dbed063bb759daff2a72bcd4e019a
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.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.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.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.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
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.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.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.dangdanggame.csmj.MainActivity	Schemes: lewan://, wx8f65419890ae05fd://,

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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

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。
2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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。
3	Activity (com.dangdanggame.csmj.wxapi.WXEntryActivity) 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。
4	Activity (com.dangdanggame.csmj.apshare.APEntryActivity) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.ACCESS_LOCATION_EXTRA_COMMANDS [android:exported=true]	警告	发现一个 Activity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: **0** | 警告: **2** | 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	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
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	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)

1	armeabi-v7a/libclinkapi-lib.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离
2	armeabi-v7a/libmain.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

3	armeabi-v7a/libtolua.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用。	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00054	从文件安装其他APK	反射	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
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	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.RECORD_AUDIO android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_FINE_LOCATION android.permission.MODIFY_AUDIO_SETTINGS
其它常用权限	6/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH

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。

URL 链接安全分析

URL信息	源码文件
• http://zxingnet.codeplex.com/ • https://api.weixin.qq.com/sns/userinfo?access_token= • http://back.hlkj123.cn/module/agency/home/AgencyHome_enter.action? • https://api.weixin.qq.com/sns/auth?access_token= • http://hotupdate.game71.net/voice/1b3e12d80v4R8BlAKIBKW4eAheTRQ.php • http://www.ascendercorp.com/ • https://go.microsoft.com/fwlink/?linkid=14202 • http://www.microsoft.com/xml/security/encryption/v1.0 • http://hotupdate.game71.net/voice/ • http://chilliant.blogspot.com.au/2012/08/srgb-aG • http://go.microsoft.com/fwlink/?linkid=14202 • https://api.weixin.qq.com/sns/oauth2/access_token?appid= • http://back.hlkj123.cn/realm/rooll/realmRooll.action?url_sign=/api/qrcode/createQrcode.action • http://scripts.sil.org/OFL • http://back.hlkj123.cn/module/pay/goods_enter.action? • http://back.hlkj123.cn/chat/room/info_1 • https://deyouyouxi.oss-cn-shenzhen.aliyuncs.com/configure/dd/init1_0.jsonhuhu-HU[illegible]anBoneId • http://back.hlkj123.cn/realm/rooll/realmRooll.action?&url_sign=/wx/circle_join/join_enter.action • https://api.weixin.qq.com/sns/oauth2/refresh_token?appid= • http://www.ascendercorp.com/typedesigners.html • https://docs.unity3d.com/Manual/Tilemap-TileAsset.html • http://www.microsoft.com/xml/security/algorithm/PKCS1-v1.5-KeyEx • http://back.hlkj123.cn/realm/rooll/realmRooll.action?&url_sign=/wx/shareRoom/shareRoomAccredit/enter.action • http://back.hlkj123.cn/realm/rooll/realmRooll.action?&url_sign=/wx/share/share_shareNewYearA.action	自研引擎-A

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
Unity	Unity Technologies	Unity 游戏使用 Il2Cpp 后端时产生的游戏代码。
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。

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

敏感凭证泄露检测

可能的密钥
6X8Y4XdM2Vhvn0KfzcEatGnWaNU=

免责声明及风险提示: