南明离火
移动应用检测平台

ANDROID 静态分析报告

消灭砖块 • v1.0

分析日期: 2024-02-23 12:54:41

应用概览

文件名称:	消灭砖块.apk
文件大小:	3.01MB
应用名称:	消灭砖块
软件包名:	com.joygame.xczk.yxjd
主活动:	cn.cmgame.billing.api.GameOpenActivity
版本号:	1.0
最小SDK:	9
目标SDK:	21
加固信息:	未加壳
应用程序安全分数:	47/100 (中风险)
跟踪器检测:	1/432
杀软检测:	25 个杀毒软件报毒
MD5:	d95cd8f25e3b6cbcaea370c627b9b26e
SHA1:	6f3868c0ee88fbcf7ee40dc1e[illegible]d51dcd01
SHA256:	829119680ec068c75e8e3[illegible]7c4f6ba27f2e3d8dbbaf[illegible]86bd36ddffa137ddddc

分析结果严重性分布

高危	中危	信息	安全	关注
4	14	1	2	2

四大组件导出状态统计

Activity组件：6个，其中export的有：1个
Service组件：1个，其中export的有：0个
Receiver组件：2个，其中export的有：2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: False
v3 签名: False
v4 签名: False
主题: C=CN, E=MGgame@chinamobile.com, ST=JS, L=Nanjing, OU=MGgame, O=CNMobile, CN=MGgame
签名算法: rsassa_pkcs1v15
有效期自: 2015-09-18 09:28:34+00:00
有效期至: 2114-09-18 09:28:34+00:00
发行人: C=CN, O=CMCA, CN=CMCA Code Signing CA
序列号: 0x16b79c2b
哈希算法: sha1
证书MD5: 86cc879de7b5050a44380ff30b829121
证书SHA1: f94b82e5e1c376b8b18008bad9eccc8eed76eee9
证书SHA256: fb2d6bfd7732fb3a65b4a23ccbc5c94a080242783634969a31cb88eeb5f9e403
证书SHA512:
0ca096f5a1974177b3ac806ee4857c4ff128b096cf55df9b46ebea854a0e9f181c6740d84ac872e72ab66c4531c3ad69855e24b60afd47d1b62daafa4b1c1360

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.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.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。
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.MODIFY_PHONE_STATE	签名(系统)	修改手机状态	允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
android.permission.GET_PACKAGE_SIZE	普通	测量应用程序空间大小	允许一个程序获取任何package占用空间容量。
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.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.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.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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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.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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.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.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入手机或 SIM 卡中存储的短信。恶意应用程序可借此删除您的信息。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
android.permission.SYSTEM_ALERT_WINDOW	危险	显示弹窗	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.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.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。

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: **1** | 警告: **0** | 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
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

本报告由南明离火移动安全分析平台生成

Manifest 配置安全分析

高危: **0** | 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 2.3-2.3.2, [minSdk=9]	警告	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。
3	Activity (com.google.sdk.GeneralActivity) 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。
4	Broadcast Receiver (com.google.sdk.PPSReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
5	Broadcast Receiver (com.google.sdk.SMSReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
6	高优先级的Intent (2147483647) [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **3** | 警告: **6** | 信息: **1** | 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	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
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	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
5	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
6	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
7	使用弱加密算法	高危	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
8	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
9	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
10	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
11	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
12	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

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	assets/libmegbpp_03.01.00_01.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。		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	False warning 符号可用

2	armeabi/libmegjb.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。		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	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	13/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.READ_PHONE_STATE android.permission.SEND_SMS android.permission.RECEIVE_SMS android.permission.READ_SMS android.permission.WRITE_SMS android.permission.GET_TASKS android.permission.SYSTEM_ALERT_WINDOW android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.READ_CONTACTS
其它常用权限	10/46	android.permission.READ_EXTERNAL_STORAGE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT

常用: 已知恶意软件经常滥用的权限。

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
oc.umeng.co	安全	否	No Geolocation information available.
u.talkingdata.net	安全	否	No Geolocation information available.
au.umeng.co	安全	否	No Geolocation information available.
www.talkingdata.net	安全	是	**IP地址:** 116.196.122.26 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
alog.umeng.co	安全	否	No Geolocation information available.
maps.google.cn	安全	否	**IP地址:** 173.194.174.94 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.40599 **经度:** -122.078514 **查看:** Google地图
gaandroid.talkingdata.net	安全	是	**IP地址:** 116.198.14.95 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
ltpy.i51fu.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• 1.1.12.1	com/a/a/v.java
• 1.1.12.1	com/a/a/y.java
• www.talkingdata.net	com/b/a/a/ac.java
• https://u.talkingdata.net/ota/b/android/dynamic/ver • https://u.talkingdata.net/ota/b/android/dynamic/sdk.zip	com/b/a/a/al.java
• http://10.10.32.105:9092/api/inAppMsg/	com/b/a/a/am.java
• 211.151.121.43 • http://gaandroid.talkingdata.net/g/d?crc=	com/b/a/a/c.java
• 10.0.0.172	com/lyhtgh/pay/g.java
• http://ltpy.i51fu.com:9820/chnlt/ltpay/failinfo.do	com/lyhtgh/pay/l.java
• http://ltpy.i51fu.com:9820/chnlt/ltpay/cancelinfo.do	com/lyhtgh/pay/m.java

• http://maps.google.cn/maps/geo?key=abcdefg&q=%s,%s	net/lazyer/util/LocationUtil.java
• 1.1.12.1 • http://oc.umeng.com/check_config_update • http://maps.google.cn/maps/geo?key=abcdefg&q=%s,%s • http://ltpy.i51fu.com:9820/chnlt/ltpay/failinfo.do • http://10.10.32.105:9092/api/inappMsg/ • http://au.umeng.com/api/check_app_update • http://alog.umeng.co/app_logs • http://ltpy.i51fu.com:9820/chnlt/ltpay/cancelinfo.do • https://u.talkingdata.net/ota/b/android/dynamic/ver • http://gaandroid.talkingdata.net/g/d?crc= • http://oc.umeng.co/check_config_update • 10.0.0.172 • http://alog.umeng.com/app_logs • http://au.umeng.co/api/check_app_update • www.talkingdata.net • https://u.talkingdata.net/ota/b/android/dynamic/sdk.zip • 211.151.121.43	自研引擎分析结果

第三方追踪器检测

名称	类别	网址
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
kiG9w0BAQUFADCBqjELMAkGA0JFSUpJTkcxEDAOBgNVBAcMB0JFSUpJTkcxFjAUBgNVB
3082022b30820194a003020102020453b946f300d06092a864886f70d01010505003 05a310d300b060355040613046c657475310d300b06035504081 3046c657475310d300b060355040713046c657475310d300b060355040a13046c657475310d300b060355040b13046c657475310d300b06035504031 3046c657475301e170d313430373036313235335a170d333930363033303132353432335a305a310d300b060355040613046c657475310d300b060 355040813046c657475310d300b060355040713046c657475310d300b060355040a13046c657475310d300b060355040b13046c657475310d300b060 355040313046c65747530819f300d06092a864886f70d010101050003818d00308190281810 0ddc3538be8bfdbaabb0a45214580d47e1759e847c549 1be44b190aa514970470307f0 4fc895839cc549f095c 747cc094afaed26a69eb3e061580c554265df2157f3ae2a0041219deefbadc71fb79df80 8ae86cbc95706a3c8b0dad7 3168bab88147a4ce7c1 7a7aea67346448c0d3f9a0649cd3084ea650203010001300d06092a864886f70d01010 505000381810093aae345f 1d327959b4f3f8f65 fbd8 9c06d7e36de26667468173364c299c2dc5fdabb4c4576adb22112956c173bcbf7e10b2e 58b48c35437a2909e 54e86135fed022e89d1 aa96136c8b280bba808e3abc146368e299714a58aac7b10d173eac494267962ee455accb 0548bdc5c3b3555 342b 2a7a
8a6fa7e4774338 73 f89a7761c332d

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。