南明离火
移动应用检测平台

ANDROID 静态分析报告

花开富贵 • v1.0.1

分析日期: 2024-06-03 15:12:13

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:	ddcea0c60cc7fd29b33d4fdadde13bb8.apk
文件大小:	26.41MB
应用名称:	花开富贵
软件包名:	com.mkdw.zhtrf
主活动:	com.bxw.hall.MainActivity
版本号:	1.0.1
最小SDK:	16
目标SDK:	25
加固信息:	未加壳
应用程序安全分数:	36/100 (高风险)
跟踪器检测:	1/432
杀软检测:	AI评估：可能有安全隐患
MD5:	ddcea0c60cc7fd29b33d4fdadde13bb8
SHA1:	1021e1d035f7b1d7539172cca[illegible]6fed3a0b
SHA256:	85445783b744943477e27[illegible]279065921d60092766[illegible]7d00e6e5b3933d4b63174a

分析结果严重性分布

高危	中危	信息	安全	关注
6	0	2	1	2

四大组件导出状态统计

Activity组件：3个，其中export的有：1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：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

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: False
v3 签名: False
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: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+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: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea3039772720179587704d89b7711292a4569

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.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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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.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.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_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。

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.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.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_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.INTERACT_ACROSS_USERS_FULL	签名	允许应用程序在所有用户之间进行交互	允许应用程序在所有用户之间进行交互。这包括在其他用户的应用程序中创建活动、发送广播和执行其他操作。
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。

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也同样存在漏洞。

Manifest 配置安全分析

高危: **3** | 警告: **2** | 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 4.1-4.1.2, [minSdk=16]	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.bxw.hall.MainActivity) 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。
4	Activity （com.bxw.hall.MainActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (25) 更新到 28 或更高版本以在平台级别修复此问题。

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

5	Activity (com.mkdw.zhtrf.wxapi.WXEntryActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (25) 更新到 29 或更高版本以在平台级别修复此问题。
6	Activity (com.mkdw.zhtrf.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。

代码安全漏洞检测

高危: **2** | 警告: **6** | 信息: **2** | 安全: **1** | 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	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
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
5	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
6	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

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

7	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
8	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
9	启用了调试配置。生产版本不能是可调试的	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
10	该文件是World Writable。任何应用程序都可以写入文件	高危	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
11	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）

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

1	armeabi-v7a/libguandu.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-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。		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	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt 两者）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项 -z,relro,-z,now 启用完整 RELRO，仅使用 -z,relro 启用部分 RELRO。	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	7/30	android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS android.permission.READ_PHONE_STATE

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

其它常用权限	9/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.BROADCAST_STICKY android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE com.android.launcher.permission.INSTALL_SHORTCUT

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
cloudaemon.com	安全	是	**IP地址:** 203.107.45.167 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161883 **查看:** 高德地图
d.appjiagu.com	安全	是	**IP地址:** 140.207.202.221 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
www.dropbox.com	安全	否	**IP地址:** 162.125.84.18 **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
mta.oa.com	安全	否	**IP地址:** 141.144.196.217 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
www.twitter.com	安全	否	**IP地址:** 104.244.42.193 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图

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

URL 链接安全分析

URL信息	源码文件
• http://scripts.sil.org/OFL • http://www.ascendercorp.com/ • http://www.ascendercorp.com/typedesigners.html • https://perf-events.cloud.unity3d.com/api/events/crashes • https://45565518-1322280293.cos.ap-beijing.myqcloud.com/app • http://www.codeplex.com/DotNetZip • http://chilliant.blogspot.com.au/2012/08/srgb-aG	自研引擎-A
• http://d.appjiagu.com/lc	com/jg/bh/Constants.java
• https://%s/api/v2/android/%s/%s	com/fm/openinstall/a/h.java
• http://1212.ip138.com/ic.asp	com/cloudaemon/lib/guandujni/GuanduJNI.java
• 111.30.131.31 • 163.177.71.186 • https://%s/api/v2/android/%s/%s • http://d.appjiagu.com/lc • 140.207.54.125 • 14.17.43.18 • http://1212.ip138.com/ic.asp • 120.198.203.175 • 123.151.152.111 • 10.0.0.172 • 10.0.0.200 • 123.126.121.167 • 103.7.30.94 • http://pingma.qq.com:80/mstat/report • 113.142.45.79 • 117.135.169.101 • 123.138.162.90 • 180.153.8.53 • http://mta.oa.com/ • http://mta.qq.com/	自研引擎-S

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

- 8.8.4.4
- 145.100.185.15
- 1.1.1.1
- www.google.com
- 103.11.143.248
- 211.233.40.78
- 119.29.107.85
- 45.77.124.64
- 136.144.215.158
- 9.9.9.9
- 176.56.236.175
- http://cloudaemon.com/howto.html#mitm
- www.dropbox.com
- 35.231.69.77
- 116.203.70.156
- 118.89.110.78
- 1.0.0.1
- 47.75.252.106
- 8.8.8.8
- 104.236.178.232
- 89.233.43.71
- 47.92.108.218
- 148.70.75.74
- 104.16.111.25
- 176.96.138.211
- 114.115.240.175
- 58.220.207.226
- 202.112.31.197
- www.facebook.com
- 145.100.185.16
- 159.69.198.101
- 131.188.3.223
- 47.101.136.37
- 131.188.3.220
- www.baidu.com:443
- 118.24.208.197
- 108.61.201.119
- 24.56.178.140
- 119.28.68.142
- 133.100.11.8
- www.twitter.com
- 127.0.0.1

lib/armeabi-v7a/libguandu.so

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

第三方 SDK 组件分析

SDK名称	开发者	描述信息
xLua	Tencent	xLua 为 Unity、.Net、Mono 等 C# 环境增加 Lua 脚本编程的能力，借助 xLua，这些 Lua 代码可以方便的和 C# 相互调用。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
sales@openvpn.net	lib/armeabi-v7a/libguandu.so

第三方追踪器检测

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

敏感凭证泄露检测

可能的密钥
openinstall统计的=> "com.openinstall.APP_KEY" : "q3lcv3"
6X8Y4XdM2Vhvn0KfzcEatGnWaNU=
n1nnGtYr7XTHiglZ5CryHflpsQO1WbeiEtYVjOv16Ypald3ftiobsPlcibYRmlGnGH4x71R9lbpTX1eMe3dndZpaAABpK5h7U5hbSrDjK1hnXefwse9wchH5ck0BoYSMv78m1hDkze2WDyuIC7QIDAQAB

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

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