南明离火
移动应用检测平台

ANDROID 静态分析报告

恋综 • v1.0.0

分析日期: 2024-04-01 20:55:35

应用概览

文件名称:	fbggcebb.apk
文件大小:	12.57MB
应用名称:	恋综
软件包名:	fgafebbc.acabaiad
主活动:	io.dcloud.PandoraEntry
版本号:	1.0.0
最小SDK:	19
目标SDK:	28
加固信息:	360加固 加固
应用程序安全分数:	40/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	9f2cc27a5196e823039e5dec34988a7f
SHA1:	8129435f384009ff07a742df875f80c87efa6207
SHA256:	ebffe059011fbd251a106c245f062d11c32e8235107633c83f4517fb02010ef35

分析结果严重性分布

高危	中危	信息	安全	关注
3	4	10	1	3

四大组件导出状态统计

Activity组件：10个，其中export的有：0个
Service组件：1个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：2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: True
v4 签名: False
主题: C=cn, ST=iaefdeih, L=edgibceg, O=jdjhejcf, OU=fdfbceee, CN=cfabffbd
签名算法: rsassa_pkcs1v15
有效期自: 2024-03-31 16:58:41+00:00
有效期至: 2124-03-07 16:58:41+00:00
发行人: C=cn, ST=iaefdeih, L=edgibceg, O=jdjhejcf, OU=fdfbceee, CN=cfabffbd
序列号: 0x5486874a
哈希算法: sha256
证书MD5: 31d4fa7652c3115d461c27c77bebf751
证书SHA1: 75eca80ad9ae97d31cd26f4daa0fd4055978dcd9
证书SHA256: 17c0ace5fde7a230ac895683ad732c7f1584ca619726bc1dc7f4270fc9cf0b6e
证书SHA512:
1fd5ea5f0117079b31c29d8f64dd6871a6d66506b30f7cf82ff67c052a5e4cd310f4b715194f0e8a09b3c3ee597947993503079534c2bd5cf02291903b104610

公钥算法: rsa
密钥长度: 1024
指纹: 6d90c2bda622e6a96dc6dd261918029592d24a036fd084cb5b2a8a32d97db2e7
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.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.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_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.INSTALL_PACKAGES	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
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。
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.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.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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.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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，离入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
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.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。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
io.dcloud.PandoraEntry	Schemes: h51eeb1ab://,

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	应用程序已使用代码签名证书进行签名

应用程序存在Janus漏洞	警告	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。

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 4.4-4.4.4, [minSdk=19]	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 Q 10、API 29 以接收合理的安全更新。
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	Activity (io.dcloud.PandoraEntry) 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 (28) 更新到 29 或更高版本以在平台级别修复此问题。
4	Activity (io.dcloud.PandoraEntryActivity) 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。
5	Activity (io.dcloud.WebAppActivity) 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。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

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/libjiagu_64.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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk', '__vsprintf_chk', '__memset_chk']	False warning 符号可用

2	assets/libjiagu_x86_64.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	True info 二进制文件有以下加固函数: ['__memcpy_chk', '__memset_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk', '__strlen_chk']	False warning 符号可用
3	arm64-v8a/libbreakpad-core.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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk']	False warning 符号可用

4	arm64-v8a/libdcblur.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	12/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_FINE_LOCATION android.permission.GET_ACCOUNTS android.permission.READ_CONTACTS android.permission.READ_SMS android.permission.SEND_SMS android.permission.WRITE_CONTACTS android.permission.WRITE_SMS android.permission.RECEIVE_SMS android.permission.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE
其它常用权限	7/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO 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

er.dcloud.io	安全	否	No Geolocation information available.
er.dcloud.net.cn	安全	是	**IP地址:** 118.89.168.191 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
ask.dcloud.net.cn	安全	是	**IP地址:** 58.222.30.203 **国家:** China **地区:** Jiangsu **城市:** Taizhou **纬度:** 32.493323 **经度:** 119.970629 **查看:** 高德地图
m3w.cn	安全	是	**IP地址:** 175.4.61.173 **国家:** China **地区:** Hunan **城市:** Zhuzhou **纬度:** 27.833330 **经度:** 113.150002 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://www.idangero.us/swiper/ • http://dev.dcloud.net.cn/mui • http://perfectionkills.com/global-eval-what-are-the-options/	自研引擎分析结果

• javascript:(function(){if(!((window.__html5plus__&&__html5plus__.isready)?__html5plus__:(navigator.plus&&navigator.plus.isready)?navigator.plus:window.plus)){window.__load__plus__&&window.__load__plus__();}var • https://er.dcloud.io/rv • 4.5.4.1 • http://localhost • javascript:(function(){var • javascript:!function(){(window.__html5plus__&&__html5plus__.isready?__html5plus__:navigator.plus&&navigator.plus.isready?navigator.plus:window.plus • https://er.dcloud.io/sc • javascript:settimeout(function(){location.__page__load__over__ • data:image/.*;base64 • https://er.dcloud.net.cn/sc • javascript:window.__neednotifynative__=true • https://m3w.cn/s/ • https://er.dcloud.net.cn/rv • 4.5.4.2 • https://localhost • data:image/png;base64 • data:text/html,chromewebdata	assets/data.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。
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。
android-gif-drawable	koral-	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。

邮箱地址敏感信息提取

EMAIL	源码文件
t@i.taj p@t.0t	assets/data.so

敏感凭证泄露检测

可能的密钥
DCLOUD的 "ApplicationId" : "plus.H56579B3B"
DCLOUD的 "CHANNEL" : "common"
DCLOUD的 "APPID" : "H51EEB1AB"
DCLOUD的 "DCLOUD_STREAMAPP_CHANNEL" : "plus.H56579B3B|H51EEB1AB|120398240508|common"
DCLOUD的 "AD_ID" : "120398240508"
w7zHlsSTZe6fiMSDbUFwcGxpY2F0aW9uSW5mb2Xun4jEg+6fiMecxJU=
w7pkxINl7p+IxINsaWJqaWFndV94ODYuc29l7p+IxIPHlMO8xIU=
7p+IYsSNZe6fiMSDU0hBMWXun4jEg2XDusSP
YsO8xIVl7p+IxINhbmRyb2lkLmFwcC5Mb2FkZWRBcGtl7p+IxIPHnMeWxIc=
x5xjxI9l7p+IxINsaWJqaWFndS5zb2Xun4jEg8eaw7zEkQ==
ZO6fiMSLZe6fiMSDLy5qaWFndS90cnkuZmxhZ2Xun4jEg2HHmsSN
x5zun4jEj2TDvMSH6K+35bCG5oKo55qE5a6J5Y2T5L+u5pS55aSn5biI6LSm5Y+35Y2H57qn5Yiw6LaF57qnVklQ5ZCO6L+b6KGM5Yqg5Zu677yM5Y2z5Y+v5Y675o6J5pys5raI5oGvZMO8xIfHmGTEkQ==
7p+IZcSRZe6fiMSDbUFwcGxpY2F0aW9uZe6fiMSDYe6fiMST
7p+IZMSNZe6fiMSDbGliamlhZ3VfNjQuc29l7p+IxINl7p+IxI8=
x5xixI1l7p+IxINtQWxsQXBwbGljYXRpb25zZe6fiMSDw7zHmsSP
w7zHmsSBZe6fiMSDZmdhZmViYmMuYWNhYmFpYWRl7p+IxIPDue6fiMSD
ZceYxIIl7p+IxINtTWFpblRocmVhZGXun4jEg8ecw7zEiw==
w7rDucSRZe6fiMSDbGliamlhZ3VfeDg2LnNvZe6fiMSDZmXEiw==
ZGHEi2TDvMSHNzVlY2E4MGFkOWFlOTdkMzFjZDI2ZjRkYWEwZmQ0MDU1OTc4ZGNkOWTDvMSHZGbEjQ==
Y2LEg2Xun4jEg2FuZHJvaWQuYXBwLkFjdGl2aXR5VGhyZWFkZe6fiMSDx5bHnMSF
w7xjxIIl7p+IxINjdXJyZW50QWN0aXZpdHlUaHJlYWRl7p+IxIPHmmTEiw==
ZsO6xJFkw7zEh+W6lOeUqOiiq+evoeaUue+8jOWNs+WwhumAgOWHumTDvMSHYmPEkw==
x5jFq8SBZe6fiMSDbGliamlhZ3VfeDg2XzY0LnNvZe6fiMSDxavHmsSD
x5hixIdl7p+IxINhbmRyb2lkLmFwcC5BY3Rpdml0eVRocmVhZGXun4jEg+6fiMeYxIk=
w7ljxI1l7p+IxINhbmRyb2lkLmNvbnRlbnQuQ29udGV4dFByb3ZpZGVyZe6fiMSDxavFq8SP
7p+Iw7nEi2TDvMSHZmdhZmViYmMuYWNhYmFpYWRkw7zEh2THlsSL
ZGPEi2Xun4jEg21Mb2NhbFByb3ZpZGVyZe6fiMSDYsWrxI0=

x5RmxIdl7p+IxIMvLmppYWd1L2xpYmppYWd1Ze6fiMSD7p+Ix5rEiQ==
ZWTEiWXun4jEgy8uamlhZ3Uvc3VjY2Vzcy5mbGFnZe6fiMSDxavun4jEiw==
Y8eYxIFl7p+IxINjb20uc3R1Yi5TdHViQXBwZe6fiMSDw7plxIM=
xavHIMSFZe6fiMSDbGliamlhZ3VfeDg2XzY0LnNvZe6fiMSDZWLEhw==
7p+Ix5bEiWXun4jEg21Qcm92aWRlck1hcGXun4jEg2VlxIs=
ZGPEh2Xun4jEg21BcHBsaWNhdGlvbmXun4jEg8eaZcSJ
ZceYxI9l7p+IxINtQ29udGV4dGXun4jEg2XHmsSR
x5bHmsSTZe6fiMSDYXR0YWNoZe6fiMSDw7xjxJU=
YsO5xIFl7p+IxINhbmRyb2lkLmFwcC5Mb2FkZWRBcGtl7p+IxINjx5zEgw==
YWTEkWXun4jEg2NvbS5zdHViLlN0dWJBcHBl7p+IxIPHlseYxJM=
ZsO5xItl7p+IxINtSW5pdGlhbEFwcGxpY2F0aW9uZe6fiMSDZMO8xI0=
x5zun4jEk2Xun4jEgy8uamlhZ3Uvc3VjY2Vzcy5mbGFnZe6fiMSDx5zun4jElQ==
YcO8xItl7p+IxINhc3NldHMvZGF0YS5zb2Xun4jEg2bun4jEjQ==
x5zFq8SFZe6fiMSDY29tLnN0dWIuU3R1YkFwcGXun4jEg2NkxIc=

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，请遵守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患。