南明离火
移动应用检测平台

ANDROID 静态分析报告

lndulge • v1.00

分析日期: 2025-03-11 12:30:23

应用概览

文件名称:	ilqx_s7ufs.APK
文件大小:	10.68MB
应用名称:	lndulge
软件包名:	cplop.izbar
主活动:	io.dcloud.PandoraEntry
版本号:	1.0.0
最小SDK:	19
目标SDK:	28
加固信息:	未加壳
开发框架:	DCloud
应用程序安全分数:	36/100 (高风险)
杀软检测:	7 个杀毒软件报毒
MD5:	b3f0bab0f9170bb1e5c11b5ef4498f00
SHA1:	8efee8cb38128cee9075b86e8a01cb8544cf9567
SHA256:	fa19395150c2cf745d36f1f995b06708bd1eaa256e70c704593d1a3d6ec2bd1d

分析结果严重性

高危	中危	信息	安全	关注
3	2	0	1	0

四大组件信息

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

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=adminl3pc7y, ST=adminl3pc7y, L=adminl3pc7y, O=adminl3pc7y, OU=adminl3pc7y, CN=adminl3pc7y
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-10 09:00:35+00:00
有效期至: 2125-02-14 09:00:35+00:00
发行人: C=adminl3pc7y, ST=adminl3pc7y, L=adminl3pc7y, O=adminl3pc7y, OU=adminl3pc7y, CN=adminl3pc7y
序列号: 0x148f6131
哈希算法: sha256
证书MD5: 9b75455b2948eff7090c2c22ec64a8f4
证书SHA1: b87cd660437084234c6720cd1522718251c338ae
证书SHA256: 77603e4a78c7c49ccf982e27c103a2d49b5d367a0a537f7a8bd6b2986b7bf4b6
证书SHA512:
878bd89359fa4d54a406c87211e2312174c4f6ca6dac687ca5b10277c1edab8d3d1af614236a16a2b65685a07cb3f6a63f4b6821f2785df1322330419a7feef85

公钥算法: rsa
密钥长度: 1024
指纹: db845bc75fb9627bd2ae2dfa010adb50c14d6269fa476baedddf2e4ec8a9a7a7
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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。
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。
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，接入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。
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.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粗略的经纬度信息，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。

可浏览的Activity组件

ACTIVITY	INTENT
io.dcloud.PandoraEntry	Schemes: h51ef821e://,

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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分析

高危: 3 | 警告: 1 | 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	Activity (io.dcloud.PandoraEntry) 容易受到StrandHogg 2.0的攻击	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。
3	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。
4	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。

安全漏洞检测

序号	问题	等级	参考标准	文件位置

行为分析

编号	行为	标签	文件
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_FINE_LOCATION android.permission.GET_ACCOUNTS android.permission.READ_CONTACTS android.permission.READ_SMS android.permission.ACCESS_COARSE_LOCATION
其它常用权限	6/46	android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE

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链接分析

URL信息	源码文件

• http://www.idangero.us/swiper/ • http://perfectionkills.com/global-eval-what-are-the-options/ • http://dev.dcloud.net.cn/mui	自研引擎-A

第三方SDK

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。
DCloud	数字天堂	libdeflate is a library for fast, whole-buffer DEFLATE-based compression and decompression.
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。

密钥凭证

可能的密钥
DCLOUD的 "AD_ID" : "129400120411"
DCLOUD的 "CHANNEL" : "common"
DCLOUD的 "ApplicationId" : "plus.H50F2B245"
DCLOUD的 "APPID" : "H51EF821E"
DCLOUD的 "DCLOUD_STREAMAPP_CHANNEL" : "plus.H50F2B245|H51EF821E|129400120411|common"
"dcloud_permissions_reauthorization" : "reauthorize"
w7rHlsSRZmTEi21BbGxBcHBsaWNhdGlvbnNlnZMSLx5jHlsSR
ZWHEg2HDucSDTUFOSUZFU1QuTU1nW7nEg8eYxavEhQ==
xavun4jEi2ZkxItkZXhFbGVtZW50c2ZkxIvDuWLEiw==
xatixI1mZMSLYW5kcm9pZC5hcHAuQWN0aXZpdHlUaHJlYWRmZMSLZmHEjQ==
YWLElWZkxIthbmRyb2lkLmFwcC5Mb2FkZWRBcGtmZMSLZMeUxIE=
Y8eYxINmZMSLaW8uZGNsb3VkLmFwcGxpY2F0aW9uLkRDbG91ZEFwcGxpY2F0aW9uZmTEi8eUw7zEgw==
x5rDusSJZmTEi3BhdGhMaXN0ZmTEi2RixIk=
x5xkxI1mZMSLbWFrZVBhdGhToGVtZW50c2ZkxIvDuceaxI0=
Ye6fiMSDZmTEi2dldEluc3RhbmNlZmTEi2ZkxIM=
YcecxJNmZMSLY8BsbBAuaXpiYXJmZMSLw7zHlMST
ZWTEjWZkxIhZXMvcmF3L2ZkxIvDusO5xI0=
ZWHEj2ZkxIttSW5pdGlhbEFwcGxpY2F0aW9uZmTEi+6fiGHEjw==

x5plxJVmZMSLamF2YXguY3J5cHRvLkNpcGhlcmZkxIvDuWbEgQ==
x5rHlsSTZmTEi21QYWNrYWdlSW5mb2ZkxItmw7zEkw==
x5jDvMSDZmTEi21BcHBsaWNhdGlvbmZkxIvFq8WrxIM=
7p+IYsSLZmTEi2phdmEuc2VjdXJpdHkuc3BlYy5BbGdvcml0aG1QYXJhbWV0ZXJTcGVjZmTEi8O5x5zEiw==
w7rDusSFZmTEi21BcHBsaWNhdGlvbkluZm9mZMSLx5TDucSF
Y8eWxIVhw7nEgzE3NDE2MjYwODE0MTBhw7nEg2Hun4jEhw==
vfdcreeun0xx5ichsq82ywf84l7krqua3cm9750wb
x5rHlsSHZmTEi2FuZHJvaWQuYXBwLkNvbnRleHRJbXBsZmTEi8eW7p+IxIc=
x5ZhxJVmZMSLYjg3Y2Q2NjA0MzcwODQyMzRjNjcyMGNkMTUyMjcxODI1MWMzMzhhZWZkxIvFq8eYxIE=
x5bHlsSFZmTEi0FFUy9DQkMvUEtDUzVQYWRkaW5nZmTEi8eWx5jEhQ==

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。