



ANDROID 静态分析报告



环境移动执法系统 v2.0.7

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

分析日期: 2024-05-06 16:03:22

i应用概览

文件名称:	05ep.apk
文件大小:	24.88MB
应用名称:	环境移动执法系统
软件包名:	uni.UNI95DC654
主活动:	io.dcloud.PandoraEntry
版本号:	2.0.7
最小SDK:	19
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	41/100 (中风险)
杀软检测:	AI评估: 很危险, 请谨慎安装
MD5:	ff540626a69ea106bd2b5319cdcc3940
SHA1:	548cc18b6f575b88aa996dff331d5233e005800e
SHA256:	4aa0ee8b802609968aef17bd80827d06bf4903ff84510ec2f9e7d08812a13c06

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✓ 安全	🔍 关注
3	5	1	1	3

📦 四大组件导出状态统计

Activity组件: 20个, 其中export的有: 0个
Service组件: 1个, 其中export的有: 0个
Receiver组件: 1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=, L=, O=Android, OU=Android,

CN=6nlyOkMQkcp8C4KbwXggjphIZQsOhnfrSDU70rW6TFzxis99KY6ympRDbP2yCJ9MlegNUXQDe5Geq7PrWxqS%2FA%3D%3D

签名算法: rsassa_pkcs1v15

有效期自: 2023-03-19 12:06:08+00:00

有效期至: 2123-02-23 12:06:08+00:00

发行人: C=CN, ST=, L=, O=Android, OU=Android,

CN=6nlyOkMQkcp8C4KbwXggjphIZQsOhnfrSDU70rW6TFzxis99KY6ympRDbP2yCJ9MlegNUXQDe5Geq7PrWxqS%2FA%3D%3D

序列号: 0x3ff8867

哈希算法: sha256

证书MD5: bc3c16229a88cf0bd995aaa130f47bc4

证书SHA1: a2fb7f5b2b8823b838e840ec8d9c875d5cc50495

证书SHA256: da5a12c8246107cf25d304fdfaea454081b44c0e931115dbaa89b89241229a3f

证书SHA512:

cfbfde519a04978c1d1db28eb228a2718127d5dab013b294b27dd6fa0817b2fb9915e47fc253b9028b26325ad0b94bd5d861f008d7113667f166f8d4d6ae24

公钥算法: rsa

密钥长度: 2048

指纹: 35a679817073ded25f85357007a7bf7b7a6083e685b1abe512266e635ba0e87

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	危险(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_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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.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_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.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.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_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.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_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角标	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”。
com.asus.msa.SupplementaryOid.ACCESS	普通	获取厂商oid相关权限	获取设备标识信息oid，在华硕设备上需要用到的权限。

🔒 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: 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

Manifest 配置安全分析

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	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 4.4-4.4.4, [minSdk=19]	信息	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 Strand Hogg 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

高危: 0 | 警告: 3 | 信息: 1 | 安全: 0 | 屏蔽: 0

序号	问题	严重程度	参考标准	文件位置
1	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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
2	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
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: In sufficient 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	arm64-v8a/liblamemp3.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shell code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。这可以通过在函数返回之前验证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 symbols stripping符号可用

2	arm64-v8a/libstatic-webp.so	<p>True info</p> <p>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 shell code 不可执行。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>No ne info</p> <p>二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>No no info</p> <p>二进制文件没有设置 RUNPATH</p>	<p>True info</p> <p>二进制文件有以下加固函数: ['_vsprintf_chk', '_strlen_chk', '_memcpy_chk', '_mmmove_chk', '_vsprintf_chk']</p>	<p>False warning</p> <p>符号可用</p>
---	-----------------------------	--	--	--	---	---	--	---

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	11/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_PHONE_STATE android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS
其它常用权限	10/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO

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
----	----	------	------

m3w.cn	安全	是	IP地址: 43.142.131.213 国家: 中国 地区: 浙江 城市: 湖州 纬度: 30.870550 经度: 120.093300 查看: 高德地图
www.android.com	安全	否	IP地址: 216.58.220.110 国家: 美利坚合众国 地区: 加利福尼亚 城市: 山景城 纬度: 37.405991 经度: -122.078544 查看: Google 地图
er.dcloud.io	安全	否	No Geolocation information available.
er.dcloud.net.cn	安全	是	IP地址: 43.142.131.213 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
lame.sf.net	安全	否	IP地址: 104.18.21.237 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
ask.dcloud.net.cn	安全	是	IP地址: 43.142.131.213 国家: 中国 地区: 江苏 城市: 台州 纬度: 32.492168 经度: 119.910767 查看: 高德地图

🌐 URL 链接安全分析

URL 信息	源码文件
<ul style="list-style-type: none"> https://github.com/emn178/js-md5 https://imgco.t.bspapp.com https://service.dcloud.net.cn/uniapp/feedback.html https://bladex.vip https://www.sxqthbkj.com/download/eps.wgt https://sns.bladex.vip https://api.bspapp.com https://www.sxqthbkj.com https://cdn.uviewui.com/uview/example/ http://mohens.com/guides/ 	自研引擎-A

<ul style="list-style-type: none"> • https://er.dcloud.net.cn/rv • https://m3w.cn/s/ • 4.5.4.1 • https://er.dcloud.net.cn/sc • https://er.dcloud.io/sc • http://www.android.com/ • https://er.dcloud.io/rv • javascript:window.__neednotifynative__=true • 4.5.4.2 	自研引擎-S
<ul style="list-style-type: none"> • http://lame.sf.net 	lib/arm64-v8a/liblamemp3.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。
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
C++ 共享库	Android	在 Android 应用中运行原生代码。
GIFLIB	GIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs since 1989. It is deployed everywhere you can think of and some places you probably can't - graphics applications and web browsers on multiple operating systems, game consoles, smartphones, and likely your ATM too.
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
android-gif-drawable	koral-	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
Weex	Alibaba	Weex 致力于使开发者能基于通用跨平台的 Web 开发语言和开发经验，来构建 Android、iOS 和 Web 应用。简单来说，在集成了 WeexSDK 之后，你可以使用 JavaScript 语言和前端开发经验来开发移动应用。
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。

敏感凭证泄露检测

可能的密钥
DCLLOUD的"AD_ID": "123052250508"
DCLLOUD的"APPID": "UNI_95DC654"
DCLLOUD的"DCLLOUD_STREAMAPP_CHANNEL": "uni.UNI95DC654 _UNI_95DC654 123052250508 common"
DCLLOUD的"ApplicationId": "uni.UNI95DC654"
DCLLOUD的"CHANNEL": "common"
"dcloud_permissions_reauthorization": "reauthorize"

"dcloud_tips_certificate": "certificate"

040965e4bda149ae0d190b8cc3c0a25d4

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

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