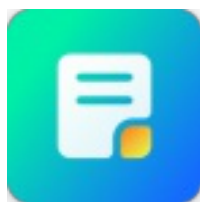




ANDROID 静态分析报告



易抓抓 • v5.3.7

分析日期: 2024-05-18 08:38:28

i应用概览

文件名称:	plus.h5600a8b1.apk
文件大小:	7.93MB
应用名称:	易抓抓
软件包名:	plus.H5600A8B1
主活动:	io.dcloud.PandoraEntry
版本号:	5.3.7
最小SDK:	21
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	52/100 (中风险)
杀软检测:	5 个杀毒软件报毒
MD5:	0b2bc35b244d32e7784f5b29b3763c03
SHA1:	e45e96add8b680fc457f0453cab58364dc161d3
SHA256:	b771654eaf891a29cf30f29d90d27163b1e8c315f943006a3d5cb3a742c4c996

分析结果严重性分布

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
1	5	1	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: False
v4 签名: False
主题: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2021-04-12 08:27:53+00:00
有效期至: 2121-03-19 08:27:53+00:00
发行人: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug
序列号: 0x363bc393
哈希算法: sha256
证书MD5: 06838cc840093b9d4689fc419ba1a3f3
证书SHA1: 97c84101b9141c130dd75d7428a2922518c36dcd
证书SHA256: b01d06180d003e79c7b9088993b8e5ae7a19b0da1161aa097c7f398a6f514fa7
证书SHA512:
67720eb20639d1f5f9c8b7b201b185ea4364f6a89bedd35aa1d273002c16d65a7739f59679510d3b96c1f2c3dd3136d9a34451cb679251a86ff4cafdc18314bf

公钥算法: rsa
密钥长度: 2048
指纹: b27ac6d7a4586417c251be6e44179616262379e57da2d1e19db0995be0ddf509
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_CHECKIN_PROPERTIES	签名(系统)	访问check-in的属性	允许对检入服务上传的属性进行读/写访问。普通应用程序不能使用此权限。
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.CONTROL_LOCATION_UPDATES	签名(系统)	控制定位更新	允许获得移动网络定位信息改变。普通应用程序不能使用此权限。

android.permission.DELETE_CACHE_FILES	签名(系统)	删除缓存文件	允许应用删除缓存文件。
android.permission.DELETE_PACKAGES	签名(系统)	删除应用程序	允许应用程序删除 Android 包。恶意应用程序可借此删除重要的应用程序。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.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.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。
android.permission.INSTALL_LOCATION_PROVIDER	签名(系统)	安装位置提供商	创建用于测试的模拟位置信息源。恶意程序可以用它来覆盖由真实位置信息源，如GPS或网络提供商返回的位置或状态，或者监视和报告您的位置到外部源
android.permission.INSTALL_SHORTCUT	普通	允许在启动器中安装快捷方式	允许应用程序在launcher中安装快捷方式。
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_CONTACTS	危险	读取联系人信息	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_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.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
android.permission.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
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_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_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。
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权限。
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”。

可浏览 Activity 组件分析

ACTIVITY	INTENT
io.dcloud.PandoraEntry	Scheme:h5600a8b1://,

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: 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
应用程序使用了调试证书进行签名	高危	应用程序使用了调试证书进行签名。生产环境的应用程序不能使用调试证书发布。

Manifest 配置安全分析

高危: 0 | 警告: 1 | 信息: 0 | 低危: 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旧更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	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。
---	--	----	--

</> 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	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
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	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	15/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.GET_TASKS android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_CONTACTS android.permission.WRITE_SETTINGS

其它常用权限	12/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_CHECKIN_PROPERTIES android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.REORDER_TASKS 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: 江西 城市: 南昌 纬度: 28.683331 经度: 115.883331 查看: 高德地图
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
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
er.dcloud.io	安全	否	No Geolocation information available.

🌐 URL 链接安全分析

URL信息	源码文件
• https://sketch.com	自研引擎-A

- https://er.dcloud.io/rv - https://m3w.cn/s/ 4.5.4.1 - https://er.dcloud.net.cn/sc 4.5.4.2 - javascript:window.__neednotifynative__=true - https://er.dcloud.io/sc - https://er.dcloud.net.cn/rv	自研引擎-S
---	--------

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。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库
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 "ApplicationId" : "plus.H5600A8B1"
DCLLOUD的 "AD_ID" : "123516190911"
DCLLOUD的 "DCLLOUD_STREAMAPP_CHANNEL" : "plus.H5600A8B1 H5600A8B1 123516190911 "
DCLLOUD的 "APPID" : "H5600A8B1"
"dcloud_permissions_reauthorization" : "reauthoriz"
"dcloud_tips_certificate" : "certificate"
0c2f0cd637405d35a4399db4d7852454b

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