南明离火
移动应用检测平台

ANDROID 静态分析报告

迪粉桌面 • v2.5.0111.66.62

分析日期: 2025-08-01 13:57:09

应用概览

文件名称:	迪粉桌面-v2.5.0111.66.62-1523.apk
文件大小:	11.93MB
应用名称:	迪粉桌面
软件包名:	com.miktone.dilauncher
主活动:	com.miktone.dilauncher.SplashActivity
版本号:	2.5.0111.66.62
最小SDK:	25
目标SDK:	32
加固信息:	360加固
开发框架:	Java/Kotlin
应用程序安全分数:	55/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	e9e320d76401fab0d5b89fc9fcbc21b7
SHA1:	9e4ffb0f6318bf140c206e53ed1807c9955fda70
SHA256:	19a4867b7581ac3152ec71ea9109ad11ad44845d361953eb2fc8051c41df1f1

分析结果严重性分布

高危	中危	信息	安全	关注
1	15	1	2	1

四大组件导出状态统计

Activity组件：14个，其中export的有： 1个
Service组件：5个，其中export的有： 2个
Receiver组件：3个，其中export的有： 2个
Provider组件：3个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=cn, ST=gd, L=hz, O=zxy, OU=zxy, CN=zxy
签名算法: rsassa_pkcs1v15
有效期自: 2017-11-14 03:54:40+00:00
有效期至: 2042-11-08 03:54:40+00:00
发行人: C=cn, ST=gd, L=hz, O=zxy, OU=zxy, CN=zxy
序列号: 0x4af59aa9
哈希算法: sha256
证书MD5: 1e1c88f0bf6d34f9cf5315d785e237c1
证书SHA1: 934f926bd1cd943ddb88a928369d849796e52a55
证书SHA256: 6a456194efcc34c8970dbafea42664d6a9398956a3e1825c0db272329a77b330
证书SHA512:
f398c911c6c9969e03a2aace25f858dbecc6b17bddd167dafe0473d1a88f840a944039b939c38a95e577ef2f817d155798d669a1879228[illegible]a1920d4a38091729

公钥算法: rsa
密钥长度: 2048
指纹: 8eb1b4fc8accb16afc12b8f6634200be598cf1226f6eb94a7d77ea2b7bc968e5
共检测到 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.MODIFY_DAY_NIGHT_MODE	未知	未知权限	来自 android 引用的未知权限。
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.DUMP	签名(系统)	获得系统内部状态	允许应用程序检索系统的内部状态。恶意应用程序可借此检索它们本不需要的各种保密信息和安全信息。
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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
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.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.SET_TIME	签名(系统)	设置时间	允许应用程序更改手机的时间。
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。
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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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.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.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
android.permission.GET_TOP_ACTIVITY_INFO	未知	未知权限	来自 android 引用的未知权限。
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.REAL_GET_TASKS	未知	未知权限	来自 android 引用的未知权限。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
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.WRITE_SECURE_SETTINGS	签名(系统)	修改安全系统设置	允许应用程序修改系统的安全设置数据。普通应用程序不能使用此权限。
android.permission.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
android.permission.INJECT_EVENTS	签名	按键和控制按钮	允许应用程序将其自己的输入活动（按键等）提供给其他应用程序。恶意应用程序可借此掌控手机。
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.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.BLUETOOTH_SCAN	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够发现和配对附近的蓝牙设备。
android.permission.BLUETOOTH_ADVERTISE	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够向附近的蓝牙设备进行广告。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
android.permission.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。

android.permission.CHANGE_WIFI_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	签名	NotificationListenerServices 需要用于系统绑定	必须是NotificationListenerService, 以确保只有系统可以绑定到。
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.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。
android.permission.BYDAUTO_MULTIMEDIA_GET	未知	未知权限	来自 android 引用的未知权限。
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.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.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.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS_COARSE_LOCATION或ACCESS_FINE_LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
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.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_CLIPBOARD_IN_BACKGROUND	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_CLIPBOARD	未知	未知权限	来自 android 引用的未知权限。
com.icoolme.android.weather.bydauto.READ_CONTENTPROVIDER	未知	未知权限	来自 android 引用的未知权限。
com.autonavi.permission.ACCESS_LOCATION	未知	未知权限	来自 android 引用的未知权限。

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	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **0** | 警告: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、Media Player 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Activity-Alias (com.miktone.dilauncher.SplashEntryActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
4	Service (com.miktone.dilauncher.MyNotificationService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
5	Broadcast Receiver (com.miktone.dilauncher.BootReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
6	Broadcast Receiver (com.miktone.dilauncher.flow.ShizukuHelper) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
7	Service (com.miktone.dilauncher.MyAccessibilityService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
8	高优先级 Intent（9999）- {3} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **1** | 警告: **7** | 信息: **1** | 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	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: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
4	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
5	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
6	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
7	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

8	使用弱加密算法	高危	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	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
10	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

应用行为分析

编号	行为	标签	文件
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限

00047	查询本地IP地址	网络 信息收集	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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	10/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.MODIFY_AUDIO_SETTINGS android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS android.permission.WRITE_SETTINGS android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE android.permission.RECORD_AUDIO
其它常用权限	13/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NOTIFICATION_POLICY android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_LOCATION_EXTRA_COMMANDS

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
xbx.zxy-soft.cn	安全	是	**IP地址:** 120.24.44.1 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://xbx.zxy-soft.cn/xbx-mobile	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Picasso	Square	一个强大的 Android 图片下载缓存库。

敏感凭证泄露检测

可能的密钥
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78

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。