南明离火
移动应用检测平台

ANDROID 静态分析报告

System Installer • v66.9

分析日期: 2025-08-04 13:56:32

应用概览

文件名称:	System Installer v66.9.apk
文件大小:	2.71MB
应用名称:	System Installer
软件包名:	lunar.calendar.moon.phase
主活动:	ap.calm.qr
版本号:	66.9
最小SDK:	27
目标SDK:	32
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	58/100 (中风险)
杀软检测:	13 个杀毒软件报毒
MD5:	ce8ec18a5634fe2798a0872fa6ed4fb2
SHA1:	87784f09b5cbd3fef65d98d99a8ce9b50436c59c
SHA256:	97cc2d2c85aee9[illegible]957548509d7128e266610c70ff6993c91ee4cb316

分析结果严重性分布

高危	中危	信息	安全	关注
0	14	0	2	0

四大组件导出状态统计

Activity组件：77个，其中export的有： 2个
Service组件：16个，其中export的有： 2个
Receiver组件：8个，其中export的有： 5个
Provider组件：5个，其中export的有： 1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: None
主题: C=DK, ST=Eldoria, L=Wintervale, O=NeuralNest, OU=Education Technology, CN=Gaspard Van de Velde
签名算法: dsa
有效期自: 2018-03-14 10:47:30+00:00
有效期至: 2045-07-30 10:47:30+00:00
发行人: C=DK, ST=Eldoria, L=Wintervale, O=NeuralNest, OU=Education Technology, CN=Gaspard Van de Velde
序列号: 0xc1487a572961ef45
哈希算法: sha1
证书MD5: 5705cff6da1f6e6c5f016ea36012b349
证书SHA1: 18627d857c975b79d92f09f586e759c4f18d3278
证书SHA256: eb938a4f60f114d294a0aafb761258f2c9f852e179d84628a8ed36bc3b099e06
证书SHA512:
3e4e3f8f8b8da25aad11fbc52a814dc80fe022749346ba43130ecad54bf950192db4fe02a3ae37eefb8b7[illegible]90ff702af681c43540824[illegible]f243835e8e3f26

公钥算法: dsa
密钥长度: 1024
指纹: 2b4a1853746d1e9facfc79d6845f5e5bf998bc9a237bcc083e2d3ac07c0db0b7
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.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.MANAGE_OWN_CALLS	普通	使呼叫应用程序能够管理自己的呼叫	允许通过自我管理的ConnectionService API管理自己的调用的调用应用程序。
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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
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_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.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.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
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）
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。

android.permission.ACCESS_ADSERVICES_TOPICS	普通	允许应用程序访问广告服务主题	这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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。
lunar.calendar.moon.phase.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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: **12** | 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、MediaPlayer 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	Content Provider (ap.calm.cjx) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。
3	Broadcast Receiver (ap.calm.Emm) 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。

4	Service (ap.calm.xl) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
5	Service (ap.calm.tw) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_TELECOM_CONNECTION_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。
6	Activity (ap.calm.cwR) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (ap.calm.Hq) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
8	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	检测到 Broadcast Receiver 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。
9	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 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。
10	Broadcast Receiver (com.mbridge.msdk.foundation.same.broadcast.NetWorkChangeReceiver) 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。
11	Broadcast Receiver (com.mbridge.msdk.foundation.same.broadcast.NetWorkChangeReceiver) 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。
12	高优先级 Intent（2494966796）-{1} 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。

本报告由南明离火移动安全分析平台生成

代码安全漏洞检测

高危: **0** | 警告: **1** | 信息: **0** | 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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	3/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.INTERNET com.google.android.c2dm.permission.RECEIVE android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE com.google.android.gms.permission.AD_ID 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。

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/756752771718/namespaces/firebase:fetch?key=AIzaSyAfZ3GCj3Wr_4cdZ8TeRPBMN_0QRgKJ_NI ）已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

敏感凭证泄露检测

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-3940256099942544~3347511713"
"google_api_key" : "AIzaSyAfZ3GCj3Wr_4cdZ8TeRPBMN_0QRgKJ_NI"

"google_app_id" : "1:756752771718:android:111f7ffee2127d99bf7f07"
"google_crash_reporting_api_key" : "AIzaSyAfZ3GCj3Wr_4cdZ8TeRPBMN_0QRgKJ_NI"

免责声明及风险提示: