南明离火
移动应用检测平台

ANDROID 静态分析报告

平安普惠 • v1.0.0

分析日期: 2025-03-11 14:31:41

应用概览

文件名称:	89q2doe0.apk
文件大小:	0.98MB
应用名称:	平安普惠
软件包名:	com.citetapirep.ginnefp.alortciv9d
主活动:	com.citetapirep.ginnefp.alortciv9d.MainActivity
版本号:	1.0.0
最小SDK:	22
目标SDK:	29
加固信息:	未加壳
开发框架:	Cordova
应用程序安全分数:	55/100 (中风险)
杀软检测:	AI评估：安全
MD5:	51408148cd84deea66be1b6f2e4ea166
SHA1:	4d88ca12dae9c636815a9dda31edfcc041476341d
SHA256:	e89c0b339100a7d4a1370a515f000b5174434119e387d63d2d74552a263e9d59

分析结果严重性

高危	中危	信息	安全	关注
1	2	0	1	0

四大组件信息

Activity组件：1个，其中export的有：0个
Service组件：0个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：1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: False
v3 签名: False
v4 签名: False
主题: C=US, O=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2023-06-20 03:35:09+00:00
有效期至: 2050-11-05 03:35:09+00:00
发行人: C=US, O=Android, CN=Android
序列号: 0x4f0d7ed3
哈希算法: sha256
证书MD5: 9870408f862a83dfa895ab832280d413
证书SHA1: df3a5e56e953b2fcb46bb3ff3d535891c8a13614
证书SHA256: 64ff296696b6e6c6a96d1c6b82d8b84c5f9d7d2df48e89d20c01ec02669cc34d
证书SHA512:
969033ce187b827a4097ed8cc7a479457ab293fc93bdc7460511f4345ffe647c0149d57965d764939c3d9f847b22f60e661d683b782e74af84f4995a796cab6a

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.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

网络通信安全

序号	范围	严重级别	描述

证书安全分析

高危: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名
应用程序容易受到 Janus 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击

MANIFEST分析

高危: **0** | 警告: **2** | 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	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。

安全漏洞检测

序号	问题	等级	参考标准	文件位置

敏感权限分析

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	2/46	android.permission.INTERNET android.permission.WRITE_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。

URL链接分析

URL信息	源码文件
• http://jsperf.com/b64tests • http://brianleroux.github.com/lawnchair/ • https://impulsive6.com	自研引擎-A

第三方SDK

SDK名称	开发者	描述信息
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。

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。