南明离火
移动应用检测平台

ANDROID 静态分析报告

LosePrivacy • v2.0

分析日期: 2024-02-21 16:48:49

应用概览

文件名称:	app.apk
文件大小:	1.66MB
应用名称:	LosePrivacy
软件包名:	b.lose.privacy.app
主活动:	b.lose.privacy.app.FullscreenActivity
版本号:	2.0
最小SDK:	15
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	64/100 (低风险)
杀软检测:	经检测，该文件安全
MD5:	e48fd0733ce6f5b20a1c0ebc6a8e34bf
SHA1:	4f5e55c3741b92ef910770fbc6787034cebc0dce
SHA256:	a3d2d45b21a7d254a327729bc758293fd81be077da8ed83e3463ab6f489906

分析结果严重性分布

高危	中危	信息	安全	关注
0	3	1	2	0

四大组件导出状态统计

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：0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

本报告由南明离火移动安全分析平台生成

v3 签名: True
v4 签名: False
主题: C=sg, ST=sgp, L=sgp, O=openpgp, OU=openpgp, CN=openpgp
签名算法: rsassa_pkcs1v15
有效期自: 2022-05-12 15:43:57+00:00
有效期至: 2022-08-10 15:43:57+00:00
发行人: C=sg, ST=sgp, L=sgp, O=openpgp, OU=openpgp, CN=openpgp
序列号: 0x1233b620
哈希算法: sha256
证书MD5: bbc220de1b081bc43f4d1b399e70a389
证书SHA1: da1da04c91272a121fe501f727e48ef97faab433
证书SHA256: 3b14576fc89af412992525f1e2c2959ff07f205e1fa2ac6cbee2478876699480
证书SHA512:
4af50c2cdd226208fed23c6679189075c6c254fc71942f707b3b6820b6ff1f570d6a31d9fcbb835611082cd0a1ada7ec434dd5aa41da6fda0b914dce0c6ce02

公钥算法: rsa
密钥长度: 2048
指纹: 82c5ee555f2495805ba7174438c8c7818437b061e134e12f48c10212413df363
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.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.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。

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: **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
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **0** | 警告: **3** | 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 4.0.3-4.0.4, [minSdk=15]	警告	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	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过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。

代码安全漏洞检测

高危: **0** | 警告: **4** | 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
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	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
4	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
5	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
6	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	3/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
loseprivacy.online	安全	否	**IP地址:** 172.67.164.36 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
loseprivacy.org	安全	否	**IP地址:** 172.67.178.16 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
loseprivacy.cc	安全	否	**IP地址:** 172.67.217.138 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://loseprivacy.org • https://loseprivacy.online • https://loseprivacy.cc	b/lose/privacy/app/AppConfig.java
• https://d.alipay.com	b/lose/privacy/app/FullscreenActivity.java

• https://loseprivacy.online • https://loseprivacy.cc • https://loseprivacy.org • https://d.alipay.com	自研引擎分析结果

第三方 SDK 组件分析

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: