南明离火
移动应用检测平台

ANDROID 静态分析报告

app_icon

LSPatch • v0.6

分析日期: 2024-06-12 15:37:03

应用概览

文件名称:	Lspatch-v0.6-402-release.apk
文件大小:	6.88MB
应用名称:	LSPatch
软件包名:	org.lsposed.lspatch
主活动:	org.lsposed.lspatch.ui.activity.MainActivity
版本号:	0.6
最小SDK:	28
目标SDK:	34
加固信息:	未加壳
应用程序安全分数:	55/100 (中风险)
杀软检测:	3 个杀毒软件报毒
MD5:	3791509716ba6e897f81f320019b1c91
SHA1:	5054ff1f663a26277cad485cc101286dd10d7910
SHA256:	520ddeca4e998d8614be8b7[illegible]12cb9edf96e743c4[illegible]a04f9cd0aac77fa

分析结果严重性分布

高危	中危	信息	安全	关注
0	1	2	1	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：2个，其中export的有：1个
Receiver组件：1个，其中export的有：1个
Provider组件：2个，其中export的有：1个

应用签名证书信息

二进制文件已签名
v1 签名: False
v2 签名: True

v3 签名: False
v4 签名: False
主题: O=LSPosed
签名算法: rsassa_pkcs1v15
有效期自: 2021-03-01 17:11:07+00:00
有效期至: 2046-02-23 17:11:07+00:00
发行人: O=LSPosed
序列号: 0x240d0a0b
哈希算法: sha256
证书MD5: e8039e8fce644b29c4355dbfefece032
证书SHA1: 091723d25447db3145cd7590ab2dbceeb3ca3e06
证书SHA256: cba01d5fc4387b8c4c74bc05e4cce7d114c12f01688926b7ac0adbeb440a167c
证书SHA512:
d7a324ac91c48182bf0c8581a04e56e22743d2f26501234f58eacb143048ad38360602856a6388b5f2feeca8902f7f6f6ae181165b910b13f181aa4f77df698b

公钥算法: rsa
密钥长度: 2048
指纹: 36ae0c35b98b9f8d0fd7dacdeb33024727a01222d1446325e752afaa976c1b8f
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.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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
org.lsposed.lspatch.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
moe.shizuku.manager.permission.API_V23	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	应用程序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: **4** | 信息: **1** | 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存在漏洞的 Android 版本上 Android 9, minSdk=28]	信息	该应用程序可以安装在具有多个漏洞的旧版本 Android 上。支持 Android 版本 => 10、API 29 以接收合理的安全更新。

2	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。
3	Service (org.lsposed.lspatch .manager.ModuleService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
4	Content Provider (rikka.shizuku.ShizukuProvider) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.INTERACT_ACROSS_USERS_FULL [android:exported=true]	警告	发现一个 Content Provider被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
5	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

代码安全漏洞检测

高危: **0** | 警告: **6** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
2	应用程序记录日志信息,不应记录敏感信息	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	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的数据的连接可能会导致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
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
5	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限

6	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
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	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

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	0/46	

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
t.me	安全	否	**IP地址:** 185.199.108.153 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
www.protocol.jar.handler	安全	否	No Geolocation information available.
goo.gle	安全	否	**IP地址:** 67.199.248.13 **国家:** 美利坚合众国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.750134 **经度:** -73.997009 **查看:** Google 地图

api.xposed.info	安全	否	**IP地址:** 185.199.108.153 **国家:** 美利坚合众国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://api.xposed.info/using.html	de/robv/android/xposed/XposedInit.java
• www.protocol.jar.handler • www.parseutil	org/lsposed/lspd/util/ClassPathURLStreamHandler.java
• https://goo.gle/compose-feedback	b7/a.java
• https://goo.gle/compose-feedback • https://t.me/lsposed • https://github.com/lsposed/lspatch	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
LSPatch	LSPosed	LSPatch fork from Xpatch. LSPatch provides a way to insert dex and so into the target APK by repackaging.
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。
Shizuku	RikkaW	Shizuku 可以帮助普通应用借助一个由 app_process 启动的 Java 进程直接以 adb 或 root 特权使用系统 API。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

敏感凭证泄露检测

可能的密钥
dbdb5cc8a6fd89bd033a1095cb7d9e6
8a8c20d[illegible]9b891cb28212ec3d18ad6c

本报告由南明离火移动安全分析平台生成

免责声明及风险提示:

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。