南明离火
移动应用检测平台

ANDROID 静态分析报告

Image & Video Date Fixer • v1.100.1

分析日期: 2025-04-11 14:14:56

应用概览

文件名称:	Image Video Date Fixer v1.100.1(1100010).apk
文件大小:	22.31MB
应用名称:	Image & Video Date Fixer
软件包名:	eu.duong.imagedatefixer
主活动:	eu.duong.imagedatefixer.activities.MainActivity
版本号:	1.100.1
最小SDK:	28
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	62/100 (低风险)
杀软检测:	AI评估：安全
MD5:	de99aa44f748ce356d8fd57f3d66fd5a
SHA1:	9748ff143d7036f04dc1cbd2bcd2f5f693d1fcf5
SHA256:	b256f4aea2f7d49f0af5640ce44d700b9f931c90186897f9c346f5fad39c61b1

分析结果严重性

高危	中危	信息	安全	关注
0	9	1	2	0

四大组件信息

Activity组件：14个，其中export的有：0个
Service组件：6个，其中export的有：1个
Receiver组件：9个，其中export的有：1个
Provider组件：2个，其中export的有：0个

证书信息

二进制文件已签名

v1 签名: False
v2 签名: False
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=LA, O=Google, OU=android, CN=youarefinished
签名算法: rsassa_pkcs1v15
有效期自: 2021-11-20 12:02:04+00:00
有效期至: 2046-11-14 12:02:04+00:00
发行人: C=US, ST=California, L=LA, O=Google, OU=android, CN=youarefinished
序列号: 0x6391bab
哈希算法: sha1
证书MD5: ffad74a28f9a8acc6c7aa33b964d303f
证书SHA1: 13501c91424608b5dca1ffc857abc173488b7784
证书SHA256: 7981162e75cd768fc2efacee773c924be0c52217a86d85c4d2a8304f2bf1c4b4
证书SHA512:
e04fa5d9c90984f0fb42e5fa17eb3e9cf1ae672dcdc431bd9b473a619f09707eec8bf8c1fb4fb47b5d53b25d0dd0019ea67e53ea96a14ba43d1af8351e3ff203

公钥算法: rsa
密钥长度: 1024
指纹: 4b7fbf2fb7595cf0883c1c9cd470e3c788f4f31c097250738afe7db5a84abf7f
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.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.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.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.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.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。
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.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
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。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
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。
eu.duong.imagedatefixer.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

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

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	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service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。
2	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。

安全漏洞检测

高危: 0 | 警告: 6 | 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
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
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	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
7	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
8	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

动态库分析

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED（裁剪符号表）
1	arm64-v8a/libperl.so	True info 二进制文件设置了NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	地址无关的可执行文件 (PIE) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用标志 -fstack-protector-all 来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

行为分析

编号	行为	标签	文件
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
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
00036	从 res/raw 目录获取资源文件	反射	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
00091	从广播中检索数据	信息收集	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
00012	读取数据并放入缓冲流	文件	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
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	3/30	android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	5/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE

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。

域名检测

域名	状态	中国境内	位置信息
twitter.com	安全	否	**IP地址:** 162.159.140.229 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

mikepenz.com	安全	否	**IP地址:** 104.21.27.65 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
jd-apps.eu	安全	否	**IP地址:** 160.153.0.74 **国家:** 美国 **地区:** 亚利桑那州 **城市:** Tempe **纬度:** 33.336079 **经度:** -111.922157 **查看:** Google 地图
t.me	安全	否	**IP地址:** 149.154.167.99 **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

URL链接分析

URL信息	源码文件
• https://t.me/picture_manager	c6/b.java
• https://plus.google.com/	g3/g1.java
• https://github.com/mikepenz/fastadapter/blob/develop/library-core/src/main/java/com/mikepenz/fastadapter/items/abstractitem.kt#l22	q5/e.java
• https://jd-apps.eu • https://t.me/picture_manager • https://play.google.com/store/apps/details?id=eu.duong.picturemanager • https://twitter.com/j_to_the_4n • https://t.me/youarefinished_mods	eu/duong/imagedatefixer/activities/MainActivity.java
• https://www.facebook.com/dyi • https://github.com/mikepenz/fastadapter • https://www.facebook.com/dyi.download • http://mikepenz.com/	自研引擎-S

第三方SDK

SDK名称	开发者	描述信息
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。

Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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。
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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
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。

邮箱

EMAIL	源码文件
info@jd-apps.eu	c6/b.java
info@jd-apps.eu	eu/duong/imagedatefixer/activities/AboutActivity.java
jdapps@wp11094986.server-he.de info@jd-apps.eu	eu/duong/imagedatefixer/activities/SendLogActivity.java
info@jd-apps.eu	eu/duong/imagedatefixer/activities/MainActivity.java

密钥凭证

可能的密钥
"library_fastadapter_authorWebsite" : "http://mikepenz.com/"
"google_api_key" : "AIzaSyDlGAmr-Ai6MVZ8HpS0kRZvaz_ZAIGWo"

GooglePlay应用信息

标题: EXIF Image & Video Date Fixer

评分: 4.5836067 **安装:** 100,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** eu.duong.imagedatefixer

开发者信息: JD Android Apps, 8291060931035277546, None, https://jd-apps.eu, info@jd-apps.eu,

发布日期: 2020年4月18日 **隐私政策:** Privacy link

关于此应用:

按正确顺序排列图片和视频！ • 同样适用于没有 EXIF 元数据的图片，例如 WhatsApp 图片。 • 还可以纠正 Instagram 或 Facebook 等内置图库中的顺序。 你是否曾将图片从一部智能手机复制到另一部？ 从云端备份下载图片，或将图片从硬盘或存储卡复制到智能手机，然后发现图片和视频在图库中完全混淆了？ 完全混淆在一起？ 图像和视频日期修复程序正是为了解决这个问题而开发的！ 也就是说，它能将您宝贵的图片和视频按照正确的时间顺序排列。 为什么会出现这种问题？ 将文件复制到智能手机后，图片和视频的文件修改日期被设置为同一个日期，即 即图片复制到智能手机的日期。 由于文件修改日期用于在图库中排序，因此图像现在会以随机顺序显示。 □ 图像和视频日期修正程序如何纠正这种情况？ 相机在图像和视频中存储元数据，对于图像，这种元数据类型称为 EXIF，对于视频，称为 quicktime。 这些 EXIF 和 qicktime 元数据包含相机型号、GPS 坐标和录制日期等信息。 图像和视频日期修复工具可使用此录制日期将文件修改日期设置为录制

日期。 这样，图库就能重新以正确的顺序显示图像。 没有元数据的图像和视频怎么办？ 如果没有 EXIF 或 quicktime 等元数据，图像和视频日期修正工具可以使用文件名中的日期（如果有的话）。 这适用于 WhatsApp 图像等。 除了修正文件修改日期外，还能保存图片和视频的 EXIF 或 quicktime 元数据。 保存。 Image & Video Date Fixer 还能做什么？ Image & Video Date Fixer 还可以根据需要更改多个图像的日期。 有以下选项可供选择： • 手动输入日期 • 为选定文件设置日期或时间 • 按天、小时、分钟或秒递增日期 • 应用时差 • 根据文件修改日期设置 EXIF 或 quicktime 元数据 Instagram、Facebook、Twitter (X) 和其他一些应用程序的信息。 有些应用程序使用创建日期对图片进行排序，遗憾的是，技术上无法更改创建日期。 不过，Image & Video Date Fixer 可以恢复排序。 为此，Image & Video Date Fixer 必须暂时将图片和视频 到另一个文件夹。在那里，它们会根据拍摄日期进行排序，然后移回原来的位置。 这是按时间顺序进行的，最旧的图像或视频在前，最新的在后。 这意味着，虽然新的创建日期是以今天的日期创建的，但它们是按照正确的时间顺序排列的。 这样，Instagram、Facebook 等网站就能以正确的顺序显示图片和视频。 免费版每次运行可修正 50 个文件。 如果每次运行需要修正更多文件，则必须购买高级版本。 此外，只有在高级版中才能更正按创建日期排序的 Facebook 和 Instagram 图库。

免责声明及风险提示: