南明离火
移动应用检测平台

ANDROID 静态分析报告

Package Explorer - v1.0

分析日期: 2025-04-30 14:56:23

应用概览

文件名称:	Stanley v1.0.apk
文件大小:	6.18MB
应用名称:	Package Explorer
软件包名:	com.yugandhar_kumar.packageexplorer
主活动:	com.yugandhar_kumar.packageexplorer.applist.AppListActivity
版本号:	1.0
最小SDK:	24
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	67/100 (低风险)
杀软检测:	4 个杀毒软件报毒
MD5:	ec24256050f3c7537492c9a6ccc96bf5
SHA1:	a43990bf8c9dbbcf2cacc9f3645b[illegible]458d910c5e6
SHA256:	0c5f0977b6bf8dfbdb4133b3e7ff500446051a62126[illegible]ce6cd900b2c6c8da2

分析结果严重性

高危	中危	信息	安全	关注
0	3	3	1	0

四大组件信息

Activity组件：6个，其中export的有：4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：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: True
v3 签名: False
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d7958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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。
com.yugandhar_kumar.packageexplorer.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览的Activity组件

ACTIVITY	INTENT
com.yugandhar_kumar.packageexplorer.details.apk.ApkDetailsActivity	Schemes: content://, file://, Mime Types: application/vnd.android.package-archive,

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: **1** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity (com.yugandhar_kumar.packageexplorer.details.apk.ApkDetailsActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。

安全漏洞检测

高危: **0** | 警告: **2** | 信息: **3** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	SHA-1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
3	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
4	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
5	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限

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
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	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

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	1/46	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。

域名检测

域名	状态	中国境内	位置信息
paypal.me	安全	否	**IP地址:** 162.159.141.96 **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
twitter.com	安全	否	**IP地址:** 162.159.141.96 **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
instagram.com	安全	否	**IP地址:** 31.13.70.174 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://github.com/material-components/material-components-android • https://github.com/JakeWharton/timber • http://tools.android.com • https://detekt.dev • http://www.reactive-streams.org • https://kotlinlang.org	自研引擎-A

• http://instagram.com/_u/ • https://github.com/%s • http://twitter.com/intent/user?screen_name=%s • https://play.google.com/store/apps/details?id= • http://m.facebook.com/	mehdi/sakout/aboutpage/AboutPage.java
• https://play.google.com/store/apps/details?id=	com/yugandhar_kumar/packageexplorer/core/utils/PackageUtilsKt.java
• https://paypal.me/xaviergouchet	自研引擎-S

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。
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 Media	Google	与其他应用共享媒体内容和控件。已被 Media2 取代。

邮箱

EMAIL	源码文件
android@xgouchet.fr	自研引擎-S

密钥凭证

可能的密钥
"android.hardware.sensor.compass" : "compass"

GooglePlay应用信息

标题: Package Explorer

评分: 4.5 **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.yugandhar_kumar.packageexplorer

开发者信息: Yugandhar Kumar, Yugandhar+Kumar, None, None, yugandharkumar05@gmail.com,

发布日期: 2023年7月20日 **隐私政策:** Privacy link

关于此应用:

Package Explorer 是一款 Android 应用程序，可简化在 Android 项目中探索和管理包的过程。 □□ 使用 Package Explorer，开发人员可以轻松浏览项目的包结构、查看和管理依赖关系以及分析包关系。它提供了一个用户友好的界面，可以方便地理解和组织代码库。 □□□ 主要特征： □ 探索项目结构：轻松导航和浏览 Android 项目的层次结构，以找到特定的代码组件。 □ 管理依赖项：访问项目中使用的依赖项的完整列表，查看和更新其版本，以及添加或删除依赖项。 □ 分析包关系：可视化包依赖关系，以识别和解决与包关系相关的问题。 □ 搜索和过滤：快速搜索项目中的特定包、文件或依赖项。 □ 提高生产力：简化包探索流程，节省开发人员的时间和精力。 Package Explorer 对于 Android 开发人员来说是一个很有价值的工具，可以帮助他们高效地探索、管理和分析项目中的包。 □□□

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。