南明离火
移动应用检测平台

ANDROID 静态分析报告

Stickers_de_pablo_escobar - v5.1.1

分析日期: 2024-05-21 21:38:21

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

应用概览

文件名称:	Stickers_de_pablo_escobar_6450569522.apk
文件大小:	26.8MB
应用名称:	Stickers_de_pablo_escobar
软件包名:	com.simplemobiletools.launcherfczcgdditi
主活动:	com.simplemobiletools.launcher.activities.MainActivity
版本号:	5.1.1
最小SDK:	26
目标SDK:	33
加固信息:	未加壳
应用程序安全分数:	60/100 (低风险)
杀软检测:	AI评估：安全
MD5:	89a7ff4a1b4c804d054d8cee8e8a616e
SHA1:	614becff481be7a1989fcb742d93b92a9a[illegible]1211
SHA256:	f90f09e08be8e2f696c6342ebd1[illegible]422[illegible]88d887ad4c335e92[illegible]de0508c4009

分析结果严重性分布

高危	中危	信息	安全	关注
0	12	2	2	0

四大组件导出状态统计

Activity组件：11个，其中export的有： 2个
Service组件：2个，其中export的有： 0个
Receiver组件：3个，其中export的有： 3个
Provider组件：1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
v3 签名: True
v4 签名: False

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

主题: C=IN
签名算法: rsassa_pkcs1v15
有效期自: 2023-06-14 09:55:01+00:00
有效期至: 2048-06-07 09:55:01+00:00
发行人: C=IN
序列号: 0x1
哈希算法: sha256
证书MD5: cd27f110915cb0248f8f764d275c7b82
证书SHA1: e2fb3fdca83ffa9b1fc2101cddc91577a0b174a2
证书SHA256: 99063fedfac345d64b76f55a252f80fa55085f29726b9884edbc53c435b13c6b
证书SHA512:
e9b4f5da1b206abcf15202dd09c84c8676004f803e4a17ace4a9d29ee7fbd15db3b855a2dc1f9520b3d71a46b3ed38410b84e737d1de8b2a9bbd0b4ec0da0b34

公钥算法: rsa
密钥长度: 2048
指纹: 68aaeaa29e7ae76801ebd9ff336d9176faf9c6d634f6285fe781134097a7f8a8
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.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（指类悬浮播放，锁屏播放）
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。恶意程序会在用户未知的情况下监视或删除。
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.BIND_APPWIDGET	签名(系统)	选择窗口小部件	允许应用程序告诉系统哪个应用程序可以使用哪些窗口小部件。具有该权限的应用程序可以允许其他应用程序访问个人数据。普通应用程序不能使用此权限
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.EXPAND_STATUS_BAR	普通	展开/收拢状态栏	允许应用程序展开或折叠状态条。

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

Manifest 配置安全分析

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

本报告由南明离火移动安全分析平台生成

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 8.0, minSdk=26]	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	Activity-Alias (com.simplemobiletools.launcher.activities.SplashActivity.Orange) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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	Activity (com.simplemobiletools.launcher.activities.SettingsActivity) 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。
5	Broadcast Receiver (com.simplemobiletools.launcher.apper.MyReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_SMS [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。
6	Broadcast Receiver (com.simplemobiletools.commons.receivers.SharedThemeReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
7	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: **5** | 信息: **2** | 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
2	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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

3	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
4	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
5	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
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
7	SHA-1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
8	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

Native 库安全加固检测

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)

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

1	arm64-v8a/libgojni.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。		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。使用选项-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	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.RECEIVE_SMS
其它常用权限	3/46	android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.BIND_APPWIDGET

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
simplemobiletools.com	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
www.simplemobiletools.com	安全	否	**IP地址:** 185.199.110.153 **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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

dabalx.org	安全	否	**IP地址:** 172.67.207.156 **国家:** 美利坚合众国 **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
mvnrepository.com	安全	否	**IP地址:** 104.26.5.216 **国家:** 美利坚合众国 **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
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:** 诺灵顿 **纬度:** 52.184460 **经度:** -0.687590 **查看:** Google 地图
goo.gle	安全	否	**IP地址:** 67.199.248.12 **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
www.gnu.org	安全	否	**IP地址:** 209.51.188.116 **国家:** 美利坚合众国 **地区:** 马萨诸塞州 **城市:** 萨默维尔 **纬度:** 42.387600 **经度:** -71.099503 **查看:** Google 地图
www.reddit.com	安全	否	**IP地址:** 67.199.248.12 **国家:** 瑞典 **地区:** Vastra Gotalands lan **城市:** Goeteborg **纬度:** 57.707409 **经度:** 11.966732 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://play.google.com/store/apps/details?id=	q7/e.java
• www.simplemobiletools.com	com/simplemobiletools/launcher/activities/SettingsActivity.java
• https://dabalx.org/cankl2k.php?key=1icyhd8bc7bfqphjemaa&user_id=	com/simplemobiletools/launcher/apper/MainScreen.java
• https://simplemobiletools.com/upgrade_to_pro	p6/b.java

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

• www.simplemobiletools.com	d7/g.java
• https://www.facebook.com/simplemobiletools • https://github.com/simplemobiletools • https://www.reddit.com/r/simplemobiletools • https://t.me/simplemobiletools • https://play.google.com/store/apps/dev?id=9070296388022589266 • https://simplemobiletools.com/ • https://simplemobiletools.com/privacy/	a/c0.java
• https://play.google.com/store/apps/dev?id=9070296388022589266	d7/f.java
• https://play.google.com/store/apps/details?id=	k8/f.java
• https://play.google.com/store/apps/dev?id=9070296388022589266	g/o0.java
• https://play.google.com/store/apps/dev?id=9070296388022589266 • https://github.com/simplemobiletools/general-discussion#how-can-i-suggest-an-edit-to-a-file • https://play.google.com/store/apps/details?id=com.simplemobiletools.thankyou • https://goo.gle/compose-feedback • https://github.com/naman14/tandroidlame • https://github.com/tibbi/androidpdfviewer • https://github.com/koral--/android-gif-drawable • https://github.com/srikanth-lingala/zip4j • https://github.com/simplemobiletools • https://play.google.com/store/apps/details?id=com.simplemobiletools.xxx.pro • https://github.com/bjoernpetersen/m3u-parser • https://simplemobiletools.com/privacy/ • https://github.com/duolingo/rtl-viewpager • https://github.com/alexvasilkov/gestureviews • https://github.com/aritraroy/patternlockview • https://github.com/robolectric/robolectric • https://simplemobiletools.com • https://github.com/jodaorg/joda-time • https://github.com/reddit/indicatorfastscroll • https://github.com/shawnlin013/numberpicker • https://www.facebook.com/simplemobiletools • https://www.reddit.com/r/simplemobiletools • https://github.com/greenrobot/eventbus • https://github.com/ravi8x/androidphotofilters • https://dabalx.org/cankl2k.php?key=1cyhd8oc7bfqphjemaa&user_id= • https://simplemobiletools.com/upgrade-to-pro • https://mvnrepository.com/artifact/org.apache.sanselan/sanselan/0.97-incubator • https://github.com/voghdev/pdfviewpager • https://github.com/armen101/audiorecordview • https://github.com/davemorrissey/subsampling-scale-image-view • https://github.com/ajalt/reprint • https://github.com/arthurhub/android-image-cropper • https://play.google.com/store/apps/details?id= • https://www.simplemobiletools.com/donate#paypal • https://github.com/penfeizhou/apng4android • https://simplemobiletools.com/ • https://github.com/grantland/android-autofittextview • https://github.com/klinker41/android-smsmms • www.simplemobiletools.com • https://github.com/googlevr/gvr-android-sdk • https://t.me/simplemobiletools • https://github.com/chrisbanes/photoview	自研引擎-S

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

第三方 SDK 组件分析

SDK名称	开发者	描述信息

Golang	Google	Go 是一种开源编程语言，可轻松构建简单，可靠和高效的软件。
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 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。

邮箱地址敏感信息提取

EMAIL	源码文件
hello@simplemobiletools.com noreply@simplemobiletools.com	自研引擎-S

敏感凭证泄露检测

可能的密钥
"authenticate" : "Tunnistaudu"
"authenticate" : "Autenticar"
"password" : "Heslo"
"authenticate" : "Autentiser"
"password" : "Password"
"authenticate" : "Autentificare"
"authenticate" : "Godkend"
"authenticate" : "Overenie"
"authenticate" : "Uwierzytelnij"
"authenticate" : "Verificare"
"password" : "Wachtwoord"
"authenticate" : "Autentikasi"
"authenticate" : "Autentifikacija"
"authenticate" : "Identifiquese"
"authenticate" : "Autentica"
"authenticate" : "Authentifizieren"
"password" : "Passwort"
"authenticate" : "S'identifier"

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

"password" : "Lozinka"
"key" : "jksdfhksdjh2342ssd"
"authenticate" : "Autentisera"
"authenticate" : "Autendi"
"authenticate" : "Authenticate"
23cf23e4c1764e7c663df2b9a36fc2e6
WVc1a2NtOXBaQzV3Y205MmFXUmxjaTVVWld4bGNHaHZibmt1VTAxVFgxSkZRMFZKVmtWRQ==
e4f4e243ff1a26a7eea22dd5badc1333
a37ad6b27306d974626c808d21c72186
38ee4c5e67d8efd6cd89925eea5da205

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。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成