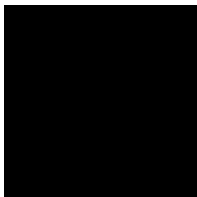




ANDROID 静态分析报告



♣ Soliq! • v46.6.361.41

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

分析日期: 2025-04-26 20:06:45

i应用概览

文件名称:	b815c02a-eb3b-4904-b18b-3c5d6867229f_Soliq! v46.6.361.41.apk
文件大小:	3.26MB
应用名称:	Soliq!
软件包名:	com.tdgbkvtqwd.fcbqgcukdeqfgtjsaoupksgvcwdjkmrdylajoky
主活动:	com.tdgbkvtqwd.fcbqgcukdeqfgtjsaoupksgvcwdjkmrdylajoky.MainActivity
版本号:	46.6.361.41
最小SDK:	26
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:	60/100 (低风险)
杀软检测:	13 个杀毒软件报毒
MD5:	652a479d3947b5d507c97677908e0a50
SHA1:	3466a7c40701a418b78bbf64a7a7af0d4ec5c470
SHA256:	fdf69be6568ba82b80c17c158b0fc621d25cfc0cde01f5d060e4d9a8f59fd475

分析结果严重性

🚫 高危	⚠️ 中危	ℹ️ 信息	✓ 安全	🔍 关注
0	12	1	2	0

四大组件信息

Activity组件: 55个, 其中export的有: 1个
Service组件: 5个, 其中export的有: 2个
Receiver组件: 10个, 其中export的有: 3个
Provider组件: 1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: True
v4 签名: False
主题: C=UZ, ST=ayvgkjedjzouohf, L=nxoucgs, O=tysmyijb, OU=tocokfwsq, CN=uyscysallrang
签名算法: ecdsa
有效期自: 2025-02-14 15:00:07+00:00
有效期至: 2052-07-02 15:00:07+00:00
发行人: C=UZ, ST=ayvgkjedjzouohf, L=nxoucgs, O=tysmyijb, OU=tocokfwsq, CN=uyscysallrang
序列号: 0xc7c6f0db6877c384
哈希算法: sha384
证书MD5: dd47544e4840cedff4039b58f627e3ea
证书SHA1: 2161597e4204f527e766e02e831fc932c8eaf5e4
证书SHA256: 93bde8a3d6214bba0c73fd8e4985335830a13d7e727444e900289baf36decf9b
证书SHA512: 8e6b6a72c040870ad1f4fe8f2e20fe6a5a1d4fb7b988aa2733289ec0cfe180239d79715dc81d547b94e95bfe36da2c0daaaeb99b35ffc2cb7082945c6426e51

公钥算法: ec
密钥长度: 256
指纹: 4cc6f221a7274015e51034011d478da597fa9136773a1797530c383c626a3456
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_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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（推送悬浮播放，锁屏播放）
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.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。
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	普通	启用特殊用途的前台服务	允许常规应用程序使用类型为“specialUse”的 Service.startForeground。
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.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。
com.tdgbkvtqwdjcdgcukdeqfgtjsaoupksgvcwdjkmrdylajom.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: 9 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	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。
2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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 (com.tdgbkvtqwd.fc bqgcukdeqfgtjsaoupksgvc wdjkmrdylajoky.Service) 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	Broadcast Receiver (com.td gbkvtqwd.fcbqgcukdeqfgtj saoupksgvcwdjkmrdylajoky Receiver) 受权限保护，但是应 该检查权限的保护级别。 Permission: android.permis sion.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。
5	Activity-Alias (com.tdgbkvt qwd.fcbqgcukdeqfgtjsaou pksgvcwdjkmrdylajoky.Hvatib anrit) 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。
6	Service (androidx.work.impl .background.systemjob.Sys temJobService) 受权限保护， 但是应该检查权限的保护级别。 Permission: android.permis sion.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。

7	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。
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallerReceiver) 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。
9	高优先级的Intent (1000) - {1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级, 应用程序有效地覆盖其他请求。

</> 安全漏洞检测

高危: 0 | 警告: 3 | 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	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
3	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
4	应用程序创建临时文件。敏感信息永远不应该被写入临时文件	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	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

⚙️ 行为分析

编号	行为	标签	文件
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
00162	创建 InetAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00026	方法反射	反射	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00104	检查给定路径是否是目录	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	5/30	android.permission.READ_PHONE_STATE android.permission.RECEIVE_SMS android.permission.CALL_PHONE android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	3/46	android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NETWORK_STATE

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。

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。
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。
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。
--------------	------------------------	--

🔑 密钥凭证

可能的密钥
c103703e120ae8cc73c9248622f3cd1e

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患。

© 2025 南明离火 - 移动安全分析平台自动生成