南明离火
移动应用检测平台

ANDROID 静态分析报告

Releam • v2.13.2

分析日期: 2025-08-04 11:36:57

应用概览

文件名称:	Releam v2.13.2-prod.apk
文件大小:	10.77MB
应用名称:	Releam
软件包名:	com.solaflashapps.releam
主活动:	com.solaflashapps.releam.ui.launch.LaunchActivity
版本号:	2.13.2
最小SDK:	23
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:	57/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	872fdab90021f5b00ed8529d1592f9c2
SHA1:	7b2b9b6c521f4a9d03239[illegible]4ce425ac5b09d69402
SHA256:	a109380ae[illegible]30df4894d4b95691f760c[illegible]7ed4d852abd48ff9fa5fccf51aa1a13c

分析结果严重性分布

高危	中危	信息	安全	关注
0	27	2	3	2

四大组件导出状态统计

Activity组件：18个，其中export的有： 8个
Service组件：12个，其中export的有： 2个
Receiver组件：13个，其中export的有： 4个
Provider组件：3个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2021-09-04 16:42:06+00:00
有效期至: 2051-09-04 16:42:06+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xf87ec9007063b830866532dcc81ea50172b6a1d9
哈希算法: sha256
证书MD5: aa77d99b0c46343acf5cce061d292ee2
证书SHA1: 66e6f09e8ebb93f685af3e68b8270f79e72cd23b
证书SHA256: c1e00b688ff340e0822548a8a5feaa362708e285276eabd38cae3fafe271fa0f
证书SHA512:
f7de4d18bf2f8683b7063899a49d20bffd8318ef36cd5813dfe1d6e6939de1d51035d55477a21a584a8bb90210f91431f1af540e7b5c7e94daa254efe9e8d8de

公钥算法: rsa
密钥长度: 4096
指纹: 74a45eccb42ba1865bcdff5e8292a62394b8e411e791cad5d9f5283f9e236b52
共检测到 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.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.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.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.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.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。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
com.solaflashapps.releam.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: **18** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
2	Activity 设置了 TaskAffinity 属性 (com.solaflashapps.releam.ui.datashare.in.TopicsImportActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
3	Activity (com.solaflashapps.releam.ui.datashare.in.TopicsImportActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
4	Activity (com.solaflashapps.releam.ui.language.LanguagesSettingsActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
5	Activity (com.solaflashapps.releam.ui.sections.SectionListActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
6	Activity (com.solaflashapps.releam.ui.words.learn.WordActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (com.solaflashapps.releam.ui.words.learn.WordPagerActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

8	Activity 设置了 TaskAffinity 属性 (com.solaflashapps.releam.instant.InstantWordCardActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
9	Activity (com.solaflashapps.releam.instant.InstantWordCardActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
10	Activity-Alias (com.solaflashapps.releam.InstantWordCardActivityProcessText) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
11	Activity 设置了 TaskAffinity 属性 (com.solaflashapps.releam.widget.WordsWidgetSettingsActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
12	Activity (com.solaflashapps.releam.widget.WordsWidgetSettingsActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
13	Broadcast Receiver (com.solaflashapps.releam.instant.BootReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
14	Broadcast Receiver (com.solaflashapps.releam.widget.WordsWidgetProvider) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
15	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

16	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
17	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
18	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **0** | 警告: **7** | 信息: **2** | 安全: **2** | 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	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	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
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
7	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
8	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
9	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
10	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
11	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

应用行为分析

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
00029	动态初始化类对象	反射	升级会员：解锁高级权限
00157	使用反射实例化新对象，可能用于 dexClassLoader	反射 dexClassLoader	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
00121	创建目录	文件 命令	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
00012	读取数据并放入缓冲流	文件	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
00104	检查给定路径是否是目录	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
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00126	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
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00010	读取敏感数据（SMS、CALLLOG）并将其放入 JSON 对象中	短信 通话记录 信息收集	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
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
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限

00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00162	创建 InetSocketAddress 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
00113	获取位置并将其放入 JSON	信息收集 位置	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	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	2/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

常用: 已知恶意软件经常滥用的权限。

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

uri.etsi.org	安全	否	**IP地址:** 172.64.147.160 **国家:** 法国 **地区:** 普罗旺斯-阿尔卑斯-蔚蓝海岸 **城市:** 索菲亚·安蒂波利斯 **纬度:** 43.622223 **经度:** 7.050000 **查看:** Google 地图
app-measurement.com	安全	是	**IP地址:** 180.163.150.166 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
pixabay.com	安全	否	**IP地址:** 172.64.147.160 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395263 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 216.58.214.14 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.150.166 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
www.solaflashapps.com	安全	否	**IP地址:** 142.250.179.211 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://goo.gl/naoooi	c4/q5.java
• https://plus.google.com/	o3/p0.java
• https://app-measurement.com/a	c4/j2.java

• https://www.solaflashapps.com/releam/privacy-policy	s8/c.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/RevocationValuesTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/OCSPValuesTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/OCSPRefTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/QualifyingPropertiesTypeImpl.java
• https://accounts.google.com/o/oauth2/revoke?token=	k3/d.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/QualifyingPropertiesDocumentImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/OCSPRefsTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/GenericTimeStampTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/OCSPIdentifierTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/ResponderIDTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/CompleteCertificateRefsTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/CertIDListTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/CRLRefTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/CRLIdentifierTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/CertificateValuesTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/CRLValuesTypeImpl.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	g3/b.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/CompleteRevocationRefsTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/CertIDTypeImpl.java

• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/CRLRefsTypeImpl.java
• https://firebase.google.com/support/privacy/init-options	v6/b.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/SignaturePolicyIdentifierTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/UnsignedPropertiesTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/UnsignedSignaturePropertiesTypeImpl.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/SignedPropertiesTypeImpl.java
• https://pixabay.com/api/	u7/l.java
• http://uri.etsi.org/01903/v1.3.2#	org/etsi/uri/x01903/v13/impl/SignedSignaturePropertiesTypeImpl.java
• https://%s/%s/%s	x6/c.java

Firebase 配置安全检测

标题	严重程度	描述信息
Firebase远程配置已禁用	安全	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/772914114629/namespaces/firebase:fetch?key=AIzaSyA0B_md-qO-PtlOocnuBUYbxe9u3EFSY2s ）已禁用。响应内容如下所示： { "state": "NO_TEMPLATE"

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Sign-In	Google	提供使用 Google 登录的 API。
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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
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。

第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"add_widget_category_key" : "add_widget_category_key"
"add_widget_key" : "add_widget_key"
"color_selection_key" : "key_color_selection"
"com.google.firebase.crashlytics.mapping_file_id" : "ddd8e8c91329415791e60bb0cfbd1933"
"dark_key" : "dark_theme"
"day_night_key" : "key_dayNight"
"file_provider_authority" : "com.solaflasharc.reham.fileprovider"
"first_language_key" : "key_first_language"
"follow_system_key" : "follow_system_theme"
"font_selection_key" : "key_font_selection"
"google_api_key" : "AIzaSyAOE_md-qO-PtlOocnuBUYbxe9u3EFSY2s"
"google_app_id" : "1:772914114629:android:68d343cfb364f13dff332c"
"google_crash_reporting_api_key" : "AIzaSyAOE_md-qO-PtlOocnuBUYbxe9u3EFSY2s"
"google_drive_export_key" : "google_drive_export_key"

本报告由南明离火移动安全分析平台生成

"google_drive_import_key" : "google_drive_import_key"
"instant_word_card_key" : "key_instant_word_card"
"large_size_key" : "Large"
"light_key" : "light_theme"
"normal_size_key" : "Normal"
"privacy_policy_key" : "key_privacy_policy"
"random_reminder_key" : "random_reminder_key"
"reminder_category_key" : "reminder_category_key"
"sd_card_cancel_store_key" : "sd_card_cancel_store_key"
"sd_card_store_key" : "sd_card_storage_key"
"small_size_key" : "Small"
"training_kind_all_key" : "all"
"training_kind_choosing_key" : "choosing"
"training_kind_interval_key" : "interval"
"training_kind_listening_key" : "listening"
"training_kind_spelling_key" : "spelling"
"training_kind_translation_key" : "description"

eyJhbGciOiJSUzI1NiIsIng1YyI6WyJNSUlDNl[illegible]UNBU293RFFZSktv[illegible]odmN[illegible]OQVFFTEJRQXdEekVOTUFzR0ExVUVBd3dFVW05dmREQWVGd
zB4TkRFeE1UZ3hOalUwTUROYUZ3MHp[illegible]TV[illegible]NeE5qVTBNRE5hT[illegible]N6QUpCZ05WQkFZVEFsVlRNUk13RVFZRFZRUUlEQXBEWVd4cFptO
XlibWxoTVJZd0ZBWURWUVFIREExT[illegible]R0ZwYmlCV2FXVjN[illegible]dZRFZRUUtEQXRIYjI5bmJHVWdTVzVqTGpFVU1CSUdBMVVFQXd3TFpt
OXZMbUpoY2k1amIyMHdnZ0VpT[illegible]cUdTSWIzRFFFQ[illegible]NElCRHdBd2dnRUtBb0lCQVFDekZWS0pPa3FUbXl5ak1IV0JPckxkcFltYzBFY
3ZHM01vaGFWK1VKclZySTJTRH[illegible]V1NrVEt6OUJLbU[illegible]QUERzMzE4NENlajliMVdleXZWQjhSajNndUgzb0wrc0pUM3U5VjJ5NHp5bzV4
TzZGV01CWUVRNlg4RGtHbF[illegible]dGhlWWJSclhORUx[illegible]MdEhUQ2FBQU5STWtPbDBORW9MYTZCUmhPRzY4Z0ZmSUF4eDVsVDhSRUU
5dXR2UHV5K3JDYUJIbmZ[illegible]BuMExTdmNl[illegible]U0lG[illegible]b1MzWTVjcmpQVmp5aVBBWlVIV25IVEZBaWxmSG5wTEJsR3hwQ3lsZVBRaE1LclBjZ3
ZEb0Q5bmQwTEE2e[illegible]EUFhYU2E4RkxPK2[illegible]DQXNGdXE5UmxmMlR0M1NqTHRXUll1aDVMdWN0UDdBZ01CQUFFd0RRWUpLb1pJ
aHZjTkFRRUxCU[illegible]FFc01BQlpsKzh[illegible]Ca3RzRHVycmk0bkYvMDdDblNCZS96VWJUaVloTXByN1ZSSURsSExvZTVsc2xMaWxmWHp
2YXltY01GZU[illegible]ndoZjdJTzdXdkl3U[illegible]K3JIeU55Z1RUaWVPMEpuOEh3KzRTQ29oSEFkTXZENXVXRXduM0x2K1c0eTdPaGFTYnpsaFZD
VkNuRkxWS2l[illegible]VhIdGRKWEpJQ[illegible]9XTk03ZzBpS1RoYWtaT3lmYjhoMXBoeTdUTVRWbFBGS3JjVkRvNW05K0dodFBDNFBOakdMb2s2
ci9qeDlD[illegible]9DYXBjcWk4ZlhKRU94S[illegible]QVlxZmpXdmh4MDBqdUVVQkhycENROHdUNFRBK0xsSTAyY1J6NXJ4VzRGUUF6MU5kb0c5SFpEWldh
K05ORl[illegible]tdFdQSk1MZCs4TDh[illegible]IiwiTUlJQzhUQ0NBZG1nQXdJQkFnSUpBTU5JMTVIckd5bGtNQTBHQ1NxR1NJYjNEUUVCQ3dVQU1BOHh
EVEFMQ[illegible]dOVkJBTU1CRkp2Y[illegible]05NVFF4TVRFNE1UWTFOREF6V2hjTk16UXhNVEV6TVRZMU5EQXpXakFQTVEwd0N3WURWUVFEREFSU2Iy
OTBNSUlCSWpBTkJna3Foa2[illegible]QkFRRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQXplVU5jNGJTV0hoT1RVKzVNUS9sT21talFXcGZCaStGSnV4dm9lT2
1Rd2k2ZnJQS0tzYUtL[illegible]Q1[illegible]QbEtFMGRtckVQOTVibmkvcUw1eEFwUDE3b3JqVWU2S1J0SkF3Rk5JNUVaYWRJZmpiaC9xKzg1QzFDcDJCUzJZbX
VaUXpYWkhQNjN5eU[illegible]Y2JNS3dDQkhYYUFnWWJtVFRrKzQrMXBqTnBIUDZZaUYyZ0NQdlNmem9rR3loYnZCcW5QYm5UZEk5dzZmak5CW
UFici91Qk9UV[illegible]rdH[illegible]sV2s1bHZzbTUxZTh2c0xTcVdob0hBRHEwQXJpQWVsVTRTSHNTQUNrUlVRU3hXVjBLNWh6VHY0ZWN2Q2JHOWRza2lE
Q3dXZyt1VFJT[illegible]pPaE9OTDAwMHE3VmV5M0RaVGNMbDgvTzROUVZhWlI1aUFnVldsV2Nzd0lEQVFBQm8xQXdUakFkQmdOVkhRNEVGZ1FV
c2ltbElS[illegible]NKUjBv[illegible]I3b004S3dIRk9IK3NJd0h3WURWUjBqQkJnd0ZvQVVzaW1sSVJEY0pSMG9mUjdvTThLd0hGT0grc0l3REFZRFZSMFRCQVV3QXdF
Qi96QU[illegible]txaGtpRzl3MEJBUXNGQUFPQ0FRRUFXUWw4U21iUW9CVjN0ak9KOHpNbGNOMHhPUHBTU05ieDBnN0VML2RRZ0pwZXQwTWNXNjJ
SSGxnUU[illegible]S2JTM1BSZW8ybnNSQi9aUnlZRHU0aTEzWkhaOGJNc0dPRVM0QlFwejEzbXRtWGc5UmhzWHFMMGVEWWZCY2pqdGxydVVieGhuQU
xwNFZOMXpWZHlXQVBDajBldTNNeHBnTVdjeW41MFFtaUpTai9FcXUvbExodmUvd0t2akc1V2huVjh1UktSdUZiRmN0MERIQUhNblpxRkhjR1M1U
28wY1luU2ZLNWZiQlJOZWxHZmxocGJiUHAwVjBhWGlxaW5xRDBZZTNPYVpkRnErMnJQMW9DL2E1L091NExzcFkzYjVvRDlyRU5keTdicTBLZXdQR
nRnUHZVa0pySjNUemJpd3ZwZ2haN3pHMjZibko1STd1YzR5MVZ1anFhT0E9PSJdfQ

8C3F193EE11A2F798ACF65489B9E6078
3071c8717539de5d5353f4c8cd59a032
470fa2b4ae81cd56ecbcda9735803434cec591fa
eWzIsJF4PExQap9HK6Vlz8DGlgGwoiLCtyOEK0Bfu
yHTAZeApn5rh6Uzfx06Gv6eHdM34YL
tgLRb4bjuZVA8xvQ9uHNs8UtpBIOiUcag2vKyfCofk5U5sNb54GgVVfxf6p4A7ObdJv1jjlUOnzR8keX5LsAM4Ia7xeqiFh0GER4l0ulVChy
W1zcp5YuPDw8mIQDVCH2uQY7qs7ejdZi5uIgIz4CbQ0wg53rWf7DDCM6MNUgZLnzNmMSMfFrpE7
7d73d21f1bd82c9e5268b6dcf9fde2cb
F1327CCA741569E70F9C18C9AF9B44B2

Google Play 应用市场信息

标题: Relearn Flashcards

评分: 4.5346537 安装: 50,000+ 价格: 0 Android版本支持: 分类: 教育 Play Store URL: com.solaflashapps.releam

开发者信息: SolaFlashApps, SolaFlashApps, None, https://www.solaflashapps.com/, solaflash@gmail.com,

发布日期: 2021年1月20日 隐私政策: Privacy link

关于此应用:

Releam 是一种创建您自己的外语学习抽认卡的简单快捷的方法。直接从互联网文章、书籍或其他应用程序添加新单词。 您可以通过以下方式创建抽认卡：— 添加应用程序本身； — 从通知面板快速添加； — 突出显示文本中的单词或短语并选择 Releam 选项， — 在 Excel 文件中构建单词列表，导入并学习单词。 添加抽认卡时，您可以： — 使用 Google 翻译 100 多种语言； — 添加您个人与所学内容相关的图像； ——添加使用示例； — 检查单词的受欢迎程度。 应用程序中已添加以下语言对的基本卡：英语、法语、德语、意大利语、日语、波兰语、葡萄牙语、俄语、西班牙语。 您可以通过即时消息、文件托

管、电子邮件或其他方式与其他人共享卡片组。导入和导出 Excel 和 Releam 文件。 使用不同类型的练习：拼写、选择答案、听力等等。使用间隔重复技术实现最有效的学习。这将有助于记忆复杂的信息。 将小部件添加到主屏幕，您的抽认卡将始终触手可及。 将抽认卡的备份保存到您的个人 Google 云端硬盘帐户。 使用主题、调色板和字体大小为您的卡片创建个性化的外观。 该应用程序无需互联网即可使用。 要改进应用程序，请写评论或将您的建议发送给我们：solaflashapps@gmail.com

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。