南明离火
移动应用检测平台

ANDROID 静态分析报告

lysa

Lysa • v2.26.2

分析日期: 2025-03-11 08:18:52

应用概览

文件名称:	Lysa v2.26.2.apk
文件大小:	13.36MB
应用名称:	Lysa
软件包名:	com.lysaapp.prod
主活动:	com.lysaapp.MainActivity
版本号:	2.26.2
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	React Native
应用程序安全分数:	46/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	5516fbad9f3503e7d646646ef3497ad0
SHA1:	59be6b5b3254b973c8f265036f2ad1ea2787e836
SHA256:	04520a167da1fd1dbe35c6d6633fb988baa2c09d9f41c8bf9451a198bfa5edc

分析结果严重性

高危	中危	信息	安全	关注
2	5	3	1	0

四大组件信息

Activity组件：3个，其中export的有：1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：1个，其中export的有：0个

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
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: 2023-05-16 14:38:34+00:00
有效期至: 2053-05-16 14:38:34+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xf8c1590a81c5604095c3df4d66708513cc00ee39
哈希算法: sha256
证书MD5: d52489c0beab4f149c58bd157b4e0e2e
证书SHA1: 584b3ce7ce741a555654a1918df5ac8725507b5b
证书SHA256: cf6b2a68e36791e10ed7a1f8906e8ee1b284bf316b9e286bbd349a656f7b2765
证书SHA512:
6f617748c5530189713e05574bc48a3cda5c97d15e9af5975495d3bdd7597cd85b5bcba489a2cf195e60752005dab766cec4f552640ef95d9800252fe3a185fd

公钥算法: rsa
密钥长度: 4096
指纹: 0efecdd1ad5ee9f83a8180292dda82457f5baf5d0c36d15ef8d379d593cf3f51
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.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.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。

可浏览的Activity组件

ACTIVITY	INTENT
com.lysaapp.MainActivity	Schemes: lysa://,

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: 1 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

MANIFEST分析

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

序号	问题	严重程度	描述信息

安全漏洞检测

高危: **2** | 警告: **4** | 信息: **3** | 安全: **0** | 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	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-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	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限
5	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
6	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
7	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限

8	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
9	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

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
00013	读取文件并将其放入流中	文件	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
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
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	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
00043	计算WiFi信号强度	信息收集 WiFi	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
00192	获取短信收件箱中的消息	短信	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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	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
00028	从assets目录中读取文件	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	0/30	
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE 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
codepush.appcenter.ms	安全	否	**IP地址:** 52.232.227.249 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 博伊顿 **纬度:** 36.667641 **经度:** -78.387497 **查看:** Google 地图
docs.swmansion.com	安全	否	**IP地址:** 172.67.142.188 **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:** 172.66.0.227 **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
pinterest.com	安全	否	**IP地址:** 172.67.142.188 **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

URL链接分析

URL信息	源码文件
• http://www.staff.science.uu.nl/ • http://www.ummulqura.org.sa/index.aspx	自研引擎-A
• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookPagesManagerShare.java
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramStoriesShare.java
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramShare.java
• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookShare.java
• https://pinterest.com/pin/create/button/?url={url}&media=$media&description={message}	cl/json/social/PinterestShare.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rngha nd led root	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java
• https://twitter.com/intent/tweet?text={message}&url={url}	cl/json/social/TwitterShare.java
• https://codepush.appcenter.ms/	com/microsoft/codepush/react/CodePush.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java

第三方SDK

SDK名称	开发者	描述信息
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。

密钥凭证

可能的密钥
"CodePushDeploymentKey" : "Shqv6tUdfKH4wTLiCPsPQF3ByPUmHhfcmasiH"
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 6
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 9
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
4843956129390645175905258525279791420276294952604174799584408071708240463528 6
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491354433653942643
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737173759623248592132296706313309438452531591012912142327488478985984
2758019355995970587784901184038904809305690585636156852142870730198868924130986086136260764883745107765459761250575
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
2661740802050217063228768716723360960729859168756973147706671368418802944094427808491545080627771902352094241225065558662157113545570916814161637315895999846
2624703509579968926862315674456698189185292349110921338781561500925518854738050089023388053975719786650872476732087
3613425095674979579858512791958788195661110667298501507197719025356841440510 9
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
4105836372515214212932612978004726840 9.144101599372555483525631403946740129 1

GooglePlay应用信息

标题: Lysa

评分: 4.7477875 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.lysaapp.prod

开发者信息: Lysa AB, Lysa+AB, None, https://lysa.se, kontakt@lysa.se,

发布日期: None **隐私政策:** Privacy link

关于此应用:

通过适合您特定需求的基金投资组合，我们希望让您能够轻松进行正确的储蓄，而难以进行错误的储蓄。 与莱莎一起，你会得到 - 基于研究的明智储蓄[1] - 具有适应风险水平的个人基金投资组合 - 精心挑选的指数基金，费用低廉 这就是它的工作原理 有了 Lysa，您的资金就有机会增长，而无需您考虑。您所要做的就是回答几个有关您想存钱的目的的问题，然后，我们会处理剩下的事情，并为您提供适合您和您的需求的广泛且廉价的基金投资组合。 1. 获取投资建议 首先回答一些有关您、您的财务状况以及您想要储蓄的问题。根据您的回答，我们会为具有适当风险水平的基金投资组合制定投资建议，并适合您的特定储蓄目标。 2. 开立账户 接受投资建议后，将自动使用该基金投资组合开设一个新的 ISK 账户。在 Lysa 开设 ISK 账户是免费的 - 您可以拥有多个不同的账户来实现不同类型的储蓄目标。 3. 自动投资 然后，当您或有将钱存入 Lysa 账户时，系统会根据账户的目标分配自动进行投资。我们还通过所谓的"储蓄"确保您的储蓄保持适当的风险和适当的利率。自动重新平衡 - 让光发挥作用 - 我们自动投资每一笔存款 - 我们不断重新平衡您的投资组合 - 我们自动将股息再投资 - 我们通过协商大幅降低您的资金成本 精选福利 - 5分钟轻松上手 - 始终免费提款和转账 - 通过ISK转移转移旧储蓄 - 邀请朋友并获得莱莎费用折扣 您身边的储蓄服务 - 单一兴趣 - 你的 金融业擅长通过多种不同的方式赚钱。在 Lysa，我们只直接从客户那里获得报酬。我们不接受任何其他人的回扣或隐藏补偿。这意味着我们只关注一个兴趣——您的。 - 费用低 研究一致认为：低费用是获得良好长期回报的关键。使用 Lysa，您只需支付约 0.4% 的低年费，比普通瑞典股票基金便宜约 70%。我们的大部分工作就是降低客户的成本。 - 基于研究 Lysa 的投资策略基于获得诺贝尔奖的研究。您的资金会自动投资于广泛且廉价的指数基金，其中包含来自世界各地的数千家公司。 - 为您量身定制 您的储蓄具有适当的风险水平是 A 和 O。根据有关您想要储蓄的几个问题，我们创建了一个 Lysa 账户，其中的基金投资组合具有适合您特定储蓄目标的适当风险水平。 -

财务安心 股市有涨有跌。随着时间的推移，我们通过自动重新平衡确保您的账户保持其风险水平。您无需考虑这一点，并且可以高枕无忧，因为您知道您的储蓄始终处于正确的轨道上。 - 像银行一样安全 通过 Lysa，您可以获得与普通银行相同的保护。您的资金将受到存款担保的保护，直到您将其投资于您拥有且与 Lysa 资产分开的基金份额为止。 关于 LYSA 的基本信息： Lysa 于 2017 年推出，该公司在斯德哥尔摩和卡尔斯克鲁纳设有办事处。 Lysa 目前为瑞典、芬兰、丹麦和德国超过 125,000 名付费客户管理着超过 250 亿瑞典克朗的资金，这使得 Lysa 成为北欧最大的独立自动储蓄服务机构。 脚注 1. Lysa的投资策略基于诺贝尔奖获得者的研究，例如强调了低费用和广泛的风险多元化对于良好的风险调整回报的重要性。

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，深入扫描软件中的潜在的漏洞和安全隐隐患。