南明离火
移动应用检测平台

ANDROID 静态分析报告

Super Wallet • v4.10.10

分析日期: 2024-07-18 14:13:25

应用概览

文件名称:	Super Wallet-4.10.10-10-release-app.apk
文件大小:	8.62MB
应用名称:	Super Wallet
软件包名:	com.super.wallet.indo
主活动:	com.pinjam.sejahtera.activity.LauncherActivity
版本号:	4.10.10
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
应用程序安全分数:	43/100 (中风险)
跟踪器检测:	2/432
杀软检测:	5 个杀毒软件报毒
MD5:	bff43e54386260fec7375ad57e6a0b08
SHA1:	cb79eef282483873095d78381ce8f94f15f94b79
SHA256:	b0fc365a23033ff15520e6eatc03dd069bb60897f83bbbb157fb6b649ca11678

分析结果严重性分布

高危	中危	信息	安全	关注
4	14	3	1	2

四大组件导出状态统计

Activity组件：21个，其中export的有：1个
Service组件：10个，其中export的有：2个
Receiver组件：4个，其中export的有：2个
Provider组件：3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: False
v4 签名: False
主题: CN=otenpol, OU=otenpol, O=otenpol
签名算法: rsassa_pkcs1v15
有效期自: 2024-06-21 03:10:23+00:00
有效期至: 2049-06-15 03:10:23+00:00
发行人: CN=otenpol, OU=otenpol, O=otenpol
序列号: 0x1
哈希算法: sha256
证书MD5: 8fc6a11ffab13a6bc446b4fd693da702
证书SHA1: a30644601f9b61391fae9a14427185a970ca9a94
证书SHA256: aa0513c78298bc984f836ca1e82bee13b664d896727cad9616638737b9d38c53
证书SHA512:
e42e21eefea2ee241ba66bae2092dddbb35b5d084292c1308f51aa92f577097797be27815764017df97b3565512c9f00b96771a[illegible]0fdfa39778ae703a53ec632

公钥算法: rsa
密钥长度: 2048
指纹: 723a8a69b544250365fbe311663e3ce44fd141c771773a32a60ebd9fea1e7357
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.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.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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.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。
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。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
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。

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.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
com.super.wallet.indo.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.pinjam.sejahtera.activity.LauncherActivity	Schemes: @string/api_scheme_url, Hosts: @string/api_scheme_host, Path Prefixes: @string/api_scheme_path,

网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

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: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) 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。

4	Service (com.pinjam.sejahtera.push.PushNewService) 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。
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。

代码安全漏洞检测

高危: **3** | 警告: **8** | 信息: **3** | 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	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
3	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
4	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

5	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
6	MD5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
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
9	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
10	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
11	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
12	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
13	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

14	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
15	该文件是World Readable。任何应用程序都可以读取文件	高危	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.READ_CALL_LOG android.permission.READ_SMS android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.CHANGE_WIFI_STATE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.c2dm.permission.RECEIVE

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
scdn-stestsettings.s	安全	否	No Geolocation information available.
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.150.33 **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
sregister.s	安全	否	No Geolocation information available.
sonelink.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
scdn-ssettings.s	安全	否	No Geolocation information available.

google.com	安全	否	**IP地址:** 172.217.26.238 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
sconversions.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.
app-measurement.com	安全	是	**IP地址:** 180.163.150.33 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.22433 **经度:** 121.46948 **查看:** 高德地图
sinapps.s	安全	否	No Geolocation information available.
aps-webhandler.appsflyer.com	安全	否	**IP地址:** 18.244.64.5 **国家:** 日本 **地区:** 大阪 **城市:** 大阪 **纬度:** 34.694218 **经度:** 135.502228 **查看:** Google 地图
sars.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.
sadrevenue.s	安全	否	No Geolocation information available.
ssdk-services.s	安全	否	No Geolocation information available.
simpression.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.
sdlsdk.s	安全	否	No Geolocation information available.
sviap.s	安全	否	No Geolocation information available.
slaunches.s	安全	否	No Geolocation information available.
goo.gl	安全	否	**IP地址:** 142.251.42.142 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图

URL链接安全分析

URL信息	源码文件

• https://%sattr.%s/api/v • https://%slaunches.%s/api/v • https://%sconversions.%s/api/v • https://aps-webhandler.appsflyer.com/api/trigger • https://%sadrevenue.%s/api/v2/log/adimpression/v6.13.1/android?app_id= • https://%svalidate.%s/api/v • https://%ssdk-services.%s/validate-android-signature • https://%sinapps.%s/api/v • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://%sadrevenue.%s/api/v2/generic/v6.13.1/android?app_id=	com/appsflyer/internal/AFi1eSDK.java
• https://%scdn-%stestsettings.%s/android/v1/%s/settings • https://%scdn-%ssettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1gSDK.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1cSDK.java
• https://%sdlsdk.%s/v1.0/android/	com/appsflyer/internal/AFf1nSDK.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFg1oSDK.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://%sapp.%s	com/appsflyer/internal/AFj1vSDK.java
• https://accounts.google.com/o/oauth2/revoke?token=	adjust/adjfa.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	iddis/nu.java
• https://%sonelink.%s/shortlink-sdk/v2 • https://%sars.%s/api/v2/android/validate_subscription?app_id= • https://%sars.%s/api/v2/android/validate_subscription_v2?app_id= • https://%sviap.%s/api/v1/android/validate_purchase?app_id= • https://%sgcdsdk.%s/install_data/v5.0/ • https://%sviap.%s/api/v1/android/validate_purchase_v2?app_id=	com/appsflyer/internal/AFe1wSDK.java

• https://%svalidate.%s/api/v • https://%scdn-%ssettings.%s/android/v1/%s/settings • https://%ssdk-services.%s/validate-android-signature • https://%sars.%s/api/v2/android/validate_subscription_v2?app_id= • https://%sviap.%s/api/v1/android/validate_purchase?app_id= • https://%sgcdsdk.%s/install_data/v5.0/ • https://%sonelink.%s/shortlink-sdk/v2 • https://aps-webhandler.appsflyer.com/api/trigger • https://%sconversions.%s/api/v • https://%s/%s/%s • https://goo.gl/naoooi • https://%sdlsdk.%s/v1.0/android/ • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://%sinapps.%s/api/v • https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps • www.google.com • https://%smonitorsdk.%s/remote-debug/exception-manager • https://firebase.google.com/support/guides/disable-analytics • https://%sadrevenue.%s/api/v2/generic/v6.13.1/android?app_id= • https://%sattr.%s/api/v • https://%slaunches.%s/api/v • https://%sadrevenue.%s/api/v2/log/adimpression/v6.13.1/android?app_id= • https://firebase.google.com/docs/analytics • https://firebase.google.com/support/privacy/init-options • https://app-measurement.com/s • https://%scdn-%stestsettings.%s/android/v1/%s/settings • https://%sregister.%s/api/v • https://google.com/search? • https://accounts.google.com/o/oauth2/revoke?token= • https://%simpression.%s • https://%sars.%s/api/v2/android/validate_subscription?app_id= • https://www.google.com • https://%sapp.%s • https://app-measurement.com/a • https://%sviap.%s/api/v1/android/validate_purchase_v2?app_id=	• 自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Jetpack Camera	Google	CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地向应用添加相机功能。该库提供了很多兼容性修复程序和解决方法，有助于在众多设备上打造一致的开发者体验。
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。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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。

第三方追踪器检测

名称	类别	网址
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
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
"api_scheme" : "superwallet"
"api_scheme_host" : "mysuperclient"
"api_scheme_path" : "/openapp"
"google_api_key" : "AIzaSyDpqYEpUDfHRVPpxnuIhS4cmjaOlIAH0o"
"google_crash_reporting_api_key" : "AIzaSyDpqYEpUDfHRVPpxnuIhS4cmjaOlIAH0o"
F8bBD0jbrvX4vN6qQN52dvxqVzrACCZ[illegible]8nykGBMp6YlamH[illegible]s9JD81TPJJuIlaAckSoKtwgpWcwS0sUFhYDnuuFzwwfAmT4=
MjViMVW1peoG7qwHaKO/weS[illegible]CGslJlXy0cTqqco=
M2OIKla4XDGg3OiAk7i[illegible]DHZ2z0oiIlgrk+8a30t8[illegible]
RPBSGC9vlgHpi[illegible]3qZp[illegible]BgebKeqPvg9g[illegible]Loj7ugppcZrmeL+ecGAyQKpRuJAMA51vPMH43n28ayg==
v45okmz[illegible]Via1xyP[illegible]6G+Kw==
N337T5Jnz[illegible]SVG0fSi1mJ5zqJAg[illegible]+p[illegible]gxK2hovU=
zxHMEut9dwACQv+CZ5[illegible]Q4[illegible]U1bW8kl88T0z9KML1D2ueAcjqs+nI4+0HjIlX/hfyiGgHUY8qB48kmi86gQ==
a0EdH7xIrLAth6[illegible]eNT[illegible]HZymrmtds2p4E0D6lg=
UKnbxPMi[illegible]UwEMRQ1HZfgrU0Ief+b9S17cJg=
682Oxh0e[illegible]Tpf/H67gav9a+WjaLopEACfZmNXd2YPA=
xaPMSZdj5B5gPk99lpaXC4TZob5JHmdrBpb8xC7tnMgwofz26BSz99O0JhZcg9gr

KnmBqoy6y6zdMQiszMB8AETAzAzdftUCtDskXdJyiVk=
dv9kom4IPNmTKNoNHPgf95svXr939X8MFj6uRDxEjG0=
MjViMVW1peoG7qwHaKO/wUUPkIkX29GfJ2nGuyC5tEY=
i12YKwjMNhavBCvsZjYsz4FNVIn7Be0LFWpQo4Q5v4k=
1/pJ+ZQVrHrQHQTxhCz0+AcQHkzndCICHKCMZK1EbVw=
zk44HY56HB7tcs07osccKtVFVEvqvV3lT99ERY4IqUI=
DRjb/tHToXhg2USxC0QXKaIztPdtQDFDuY8kMmvVZAE=
NRLiIrt08PUxW3biZiytzwifVpzBMGdy/ksk7MUXCPE=
4cfzW2T4Gbb1jFJZCL3LJqxcn4hALQ1Rd4sG1761xUo=
t2zpaWoXuysvAWjP6499VycBliOnkI5JgvoX4kgmY89B5diKooXVUHd66Dw3yWapHGafJEVhrfQFsfWiapLUbw==
gKcaJ06twoo8CfC2VtMTswtahtvbOzqTlcgk6qMU4Dw=
5QFQxt9E+wQ5IeVNpwDtMjycyPwnIhEO3u+MDqbYorc=
L0R7w7pdgYrKsmP2HCcoBUFhsS2t5hTcn9iqZQKd28g=
6yIwz18/WjZ34SD5cEwezljGbVqhdWrAnR7RjPnaLU0=
r/y9is5lm7xx+JidFXbe14s+72hsFT7IkoD+iWqEtZlNjgLHtXb8XSlGBMo0Pssq
2jEk2ZDSndvgX6m6dvNiPvMP/7xDXaBYyOO7TVdzqZw=
lVzD9nIKFq9cF5/yvvILmx3cvKBouM2coJLkklEuMp83Bcj4mHIF+OCeacrkGUDbpo6QTNpMlY25Cmst+7cM7rHLZs6Uag80EeD9mk2dPo=
AErDpRafSYBPVk9lUu1NWw==
F8bBD0jbrvX4vN6qQN52dlRkIKlNHCf2b3idvgt3yJM09Y14M5Ap5L/TNglPl1zc
ggMU7Xfw283bL5xK6c2oQ5GEFGRuH2j81BvIKXnv7E=
p614Jx4ylYteFJCLR3B5qHIWjYYqutdWh4abe8mZwW4=
VfslSvdhLKoHMt++WWR47m6U4eTXXbqw+caIIYmjauc=
V9slfieDI9LxJhUdFWB2NWXa/kxgJ9vdWx+7IgdIw=
jJfGgMqSH7Z7UuaVQFXqbQyVi3ziwMamfiuK7totcO8T1ZgqV++3c8UOXoSH61zu2SzL2lLgwzcZsYcrkSlan1peaN+ieiNv6iWzMuMZs7Lq72JePP12X8SDpW6uQ0pnV9L+z5Pjow8JY39FHpHmPXLDxQNNRfXZOWS1qHteEBJLPAV82dZLM8USkEqauFquzYTxhWL15dqDtpKyLksA==
ngs5LYbA4DgqHp/HMSRx0kodL2gXnx4vOmsemnjPAM=
G1znXzVkIGGXJBKuXTnKqbNScOQ+EfYVa4KmlZ7OlY=
iic0ivvi1kKqmS0QEbrUqacMpZJhS6ZPxycrzchJM0=
uHDag72AUDXXvRHKAFp672VMvOiC1JqiyIgPvfonZfQ=
AAmfBPwsPPtx0Xvai5gYhChMNtT/8VBsQ9IMCh8VAHAWAUhBJGAMRESks1bKvWMJ
6GMqRQYS6Cq+VYBI5UptWfwk0l1RE5vcg7YzEVuJxTc=

本报告由南明离火移动安全分析平台生成

RaZrrTQ35oHX/LLy+8m+FP7jtmqzG2kmGqhWOHICPfI=
Y8lnnNBgXogiIDBYOIW3jqZDJq+mwOexu7rPfRKR4R0=
q0WY588U6WYy1cXMbiTZA60mzcHZdhzoPO1LFkfBO9jCz8J2BqZLFTAic0EwJ8u4
lDoCljsdrfzwnD0VhQAvuQRznKUHFoEK4XPTeOA9jIrBc24FKpURKW59OyYxh5Eh
t4RzW7+rHcGI30CPy8wJBA==
tP2+GgbIyDbNl6bWO+5sN6+qUDK3HM0DF4uQo/xvrrA=
O3T7NXeuSZjlA2p0rgmS15cLdWA209d6eA/rYUbIYnY=
6lhzuQV7ca5338oO3yGyfCF2h4Xb8WnfRK/skDoACu8=
336EMdkc03IEvfKENBdD9F5U9fDzgo7JO8oF61HKzu4=
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
XeP6Ddlp/fMsq5rFT9wNZg==
682Oxh0eGSuTpf/H67gav9hLKGxnzkd4GcxvjX+hNHE=
F8bBD0jbrvX4vN6qQN52dIRkIKlNHCf2b3idvgu3vjPcdml55JkbBCTrxGRXT6Nl
wwHLL3lFmG4UJJ9GY+QN0XIUyH4c3UpzvGxiLnexHXA=
CEoklMlHcQPOHfCeqSInL0Nu4UUgefPGrQTqiSBNQ0w=
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46[illegible]8C6[illegible]FAE7212
X39QaZO0+rFQVawVpCdK2A3em/a7Fl2Sol1EagrABKU=
ktmrDep15ocBpZS2wc3bx8Izn6kMaVyJwtv4/5sQLQ4=
85WEJEmKvd7lHcAYjm/YPHuZmrBCxt3k6DjP[illegible]vhOn7Y=
yaURxTXay/Q9gzh9vcd8+0FtpeWC2n8d5SDfvaVRoM8=
lrwwaITcEhacCmH8lgbOkfV7gceyhaCC9PSnVfdp5UuNLr54Kj3KVZTnd7q9n1Ss
3BAF59A2E5331C30675FAB35F[illegible]5F[illegible]F0D116142D3D4664F1C30B804068B40614F
NKNJcW8njvwOFzKqnd+SVicWY33s99nM05eSKnSyptI=
GtInFItKtay460Rh[illegible]SvtsaGYwHAjCF5zqZn54UVlsSg=
K7biWN6oee69RU1vqbBVTlnTBm3WUcZ[illegible]Xf0SorHy6Y2/4IfWnbXtOf6Qns4BEz3
oKGIzfxObvtJy1QaYY83ZDOIltO2a[illegible]HyS+3wgOBmuI94AgTgvl7eZHamledaUDol
e3CU0Yjmx7Oegckm/Rt8dp9iNx4Fgi2Ued5j6BLJBns=
4CM5cLn7roIy[illegible]X[illegible]0/Q==
mOoUs0d[illegible]B7BIKeEcgHAVfSBqjDdZN/gw8OYSR8mCF3dxuIUrzDtWfqgjyfKjz+8
dPhqsfGTY7SL7zfb+zEN/BMB6WnC76y6CcS1tz04hev7SvTGFxtogpVU1AIz6g6c
ex1ytEuqnzpExqzXpDUSdxMY99yF10WIXZAyoVG/go4=

本报告由南明离火移动安全分析平台生成

tD+gUxO8C0964D7qA/3HD694iqIGLDHtEsZ6tszvTYA=
2ieBkREEultXNcfpdQSmoc5aZnfd8cRk4XCXG5y0bfuoP4far+5r2fAkTG2fgqSP
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
kqDatOD64eoknzEs1wvxHRh1vptA3Kha1+NoZGFirgQ=
tpj9155XrrxkGocL7CpZZrMHj3K2Qh/iAHjRkzuAAAg=
Y8lnnNBgXogilDBYOIW3jlfHTSZeqasCbGfxs7odGPQ=
eU0uK4Q3+0Rs59U0UCOa9WoNl75sfNsYthSFHUyHjJE=
ZS8ueyFkXg5LmQvHLWttHS5G6EZydmZ5xNdBxQOpmsM=
tsmmw7e+zVgwePZbLLodOXigad3sifpXx4WanQu8Taw=
maD0GjWtAFS/MmD8d4cLFMcixE4WhUuTghqIDvL5JQU=
EkXJ9gMYnLso1oRJy/BANrMhSq1u8ITlUqwE4DBm4AE=
KSm3Vxtth95KC+RpibUrSQyTs7voOzAtaqy7C4RcFEotHDqWfXU3TwUIPC+KuRW5A+hDCWRTfPr6uM5L7bg==
K0g8rknlp5Kpvja8MMCswxnN8PvW9BGT2fukpeXbOjc=
jyHxxHcZFiBj2mQkWIGYmUFB+pme5c7aWQWO/1V2aBY=
Knfj1AH7wPFLCEitcob/G3CtayEgMuamfNL+1z3k1Rc=
GjG/04qm1JdUlXxeIKByi950oBlV+e6tOL3i7uetxBQ=
z4dipYcBsOofBe53Sm4x3/ambaxqoywU5T0ZSZi9l6M=
F8bBD0jbrvX4vN6qQN52dmuM8uiZvh/QNjv4H5aYkdE=

Google Play 应用市场信息

标题: Super Wallet-Pinjaman kilat

评分: 4.6855693 **安装:** 50,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.super.wallet.indo

开发者信息: Super Wallet LLC, Super+Wallet+LLC, None, https://superwalletcompany.com/, bm0113030@gmail.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

KSP 在线贷款产品 在线现金贷款：IDR 2,000,000 - 7,000,000 贷款期限：91-180天 最高年利率（APR）：15%/年（0.04%/天） 没有其他额外费用 例子： 如果用户选择贷款金额为IDR 2,000,000，期限为150天（5个月） 那么每天必须支付的利息费用为： 2,000,000 * 0.04% = 800 卢比 每月必须支付的利息费用为： 2,000,000 * 0.04% * 30 = 24,000 印尼盾 每月付款总额为： 2,000,000 / 5 + 24,000 = 424,000 印尼盾 贷款期150天结束后，贷款总利息成本为（不含其他费用）： 2,000,000 * 0.04% * 150 = 120,000 印尼盾 150天贷款期结束后，需支付的金额为： 2,000,000 + 120,000 = 2,120,000 印尼盾 以上数字和例子均来自合作机构，Uang Bagusbu并不承诺其用户将获得100％的贷款，超级钱包是一个旨在向用户推荐值得信赖的借贷机构的金融服务平台。请注意，超级钱包本身不提供直接借贷服务；用户能否成功获得贷款将取决于所选机构的审批标准。作为一个负责任的金融平台，我们致力于不断寻找更安全、更多样化的金融产品来满足您的各种需求。 Super Wallet旨在为用户提供更加便捷的PT.Super Wallet Indonesia会员注册服务，帮助PT.Super Wallet Indonesia会员获取资金。 成为 Eka Setia Nusantara 储蓄和贷款合作社成员的要求： 1、遵守并遵守公司章程、章程及合作社管理层的决定。 2、能够维护和维护合作社的良好声誉。 超级钱包主要特点： 1.按照填写个人信息流程申请网贷。只需正确填写您的身份信息，用户就有机会获得超级钱包资金。 2、遵守印度尼西亚适用法规，确保用户信息的安全和隐私。未经贷款用户许可，数据不会泄露给第三方，如果用户长期未使用该应用，我们将删除该用户的用户信息。 3、如果用户保持良好的信用，我们保证下次贷款会更容易、更高，为用户提供智能信贷服务。 贷款申请要求如下： 1. 持有KTP的印尼公民 2. 年龄18-55岁 3. 有效手机号码 4.注册成为PT.Super Wallet Indonesia会员可以提高用户申请的批准率。 如何申请KSP机构贷款： 1. 在 Google Play 商店下载 Safe Money 应用程序 2. 填写用户资料，告诉我们用户是谁，并评估风险 3.等待审核 4、审核通过后，等待用户借贷资金入账 如果用户需要进一步的信息，可以通过以下方式联系我们： 邮箱：bm0113030@gmail.com 地址：Sunrise Garden Jl. 班让 RT.15/RW.7，北凯多亚区。 KB。印度尼西亚雅加达特区西雅加达杰鲁克市，邮编 11520

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。