



## ANDROID 静态分析报告



虚空风暴 • v2.3.2

分析日期: 2025-04-04 12:47:56

i应用概览

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| 文件名称:     | 虚空风暴 v2.32.apk                                                   |
| 文件大小:     | 41.78MB                                                          |
| 应用名称:     | 虚空风暴                                                             |
| 软件包名:     | com.mx.xkfb.vivo                                                 |
| 主活动:      | com.mxsdk.ui.activity.MHPerActivity                              |
| 版本号:      | 2.32                                                             |
| 最小SDK:    | 21                                                               |
| 目标SDK:    | 30                                                               |
| 加固信息:     | 未加壳                                                              |
| 开发框架:     | Java/Kotlin                                                      |
| 应用程序安全分数: | 46/100 (中风险)                                                     |
| 跟踪器检测:    | 3/432                                                            |
| 杀软检测:     | 经检测，该文件安全                                                        |
| MD5:      | f00ab86aa2be96eb87dcf96132973da2                                 |
| SHA1:     | 2675303eb1ed9e993de483a6687f457949695f8f                         |
| SHA256:   | 212e970c273f7da22bde9113f3b54eaadf34e1bacef05a1373a60e3e59c96c9e |

分析结果严重性分布

|      |       |       |      |      |
|------|-------|-------|------|------|
| 🚨 高危 | ⚠️ 中危 | ℹ️ 信息 | ✓ 安全 | 🔍 关注 |
| 5    | 22    | 2     | 2    | 17   |

四大组件导出状态统计

|                                |
|--------------------------------|
| Activity组件: 30个，其中export的有: 7个 |
| Service组件: 0个，其中export的有: 0个   |
| Receiver组件: 1个，其中export的有: 1个  |
| Provider组件: 1个，其中export的有: 1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: C=86, ST=guangdong, L=guangzhou, O=kaola, OU=kaola, CN=kaola  
 签名算法: rsassa\_pkcs1v15  
 有效期自: 2018-01-09 11:04:07+00:00  
 有效期至: 2117-12-16 11:04:07+00:00  
 发行人: C=86, ST=guangdong, L=guangzhou, O=kaola, OU=kaola, CN=kaola  
 序列号: 0x27454a5e  
 哈希算法: sha256  
 证书MD5: 47d4276c1a6a3839c67aad971b20a2e4  
 证书SHA1: e05e7e4fd4e556a490406959ca19fb3fae44dd3e  
 证书SHA256: 7ef6e25b0a9fd2619ee238d44fc8290897b21adfc5a33c21b60e2473d6a71eb2  
 证书SHA512:  
 6aebf8ddb3e0357c045513ea6c39e0deff3dcf7fca60ac6942f6cd283ae3000628babd1c07448501fee9f07662fca0b97a1545b562c071a5550b178ca50f2ad4

公钥算法: rsa  
 密钥长度: 2048  
 指纹: c1e19591a699b3cce733d8050a52c809e6111a7297c4ca18ae9c7faf5e2ee2c1  
 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.GET_TASKS              | 危险   | 检索当前运行的应用程序    | 允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。                      |
| android.permission.REORDER_TASKS          | 危险   | 对正在运行的应用程序重新排序 | 允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。                              |
| 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.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.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.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.CHANGE_NETWORK_STATE   | 危险   | 改变网络连通性        | 允许应用程序改变网络连通性。                                                         |
| 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。                                                        |
| android.permission.READ_LOGS              | 危险   | 读取系统日志文件       | 允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。 |

|                                             |    |              |                                                      |
|---------------------------------------------|----|--------------|------------------------------------------------------|
| android.permission.SYSTEM_ALERT_WINDOW      | 危险 | 弹窗           | 允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。                           |
| android.permission.WRITE_APN_SETTINGS       | 危险 | 写入访问点名称设置    | 允许应用程序写入访问点名称设置。                                     |
| com.asus.msa.SupplementaryDID.ACCESS        | 普通 | 获取厂商oaid相关权限 | 获取设备标识信息oaid，在华硕设备上需要用到的权限。                          |
| freemme.permission.msa                      | 未知 | 未知权限         | 来自 android 引用的未知权限。                                  |
| 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.READ_PHONE_NUMBERS       | 危险 | 允许读取设备的电话号码  | 允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。 |
| android.permission.MODIFY_AUDIO_SETTINGS    | 危险 | 允许应用修改全局音频设置 | 允许应用程序修改全局音频设置。如音量。多用于消息语音功能。                        |
| vivo.game.permission.OPEN_JUMP_INTENTS      | 未知 | 未知权限         | 来自 android 引用的未知权限。                                  |
| android.permission.REQUEST_INSTALL_PACKAGES | 危险 | 允许安装应用程序     | Android8.0 以上系统允许安装未知来源应用程序权限。                       |
| 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。    |

可浏览 Activity 组件分析

| ACTIVITY                           | INTENT                                                                |
|------------------------------------|-----------------------------------------------------------------------|
| w1.MainActivity                    | Schemes: cc://,<br>Hosts: arpgw1,                                     |
| com.vivo.unionsdk.ui.UnionActivity | Schemes: vivounion://,<br>Hosts: union.vivo.com,<br>Paths: /openjump, |

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   | 应用程序使用代码签名证书进行签名 |

Manifest 配置安全分析

高危: 0 | 警告: 11 | 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<br>[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  | 应用程序具有网络安全配置<br>[android:networkSecurityConfig=@xml/network_security_config]                              | 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  | 应用程序数据存在被泄露的风险<br>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。                                                                               |
| 4  | Broadcast Receiver (com.bytedance.applog.collector.Collector) 未被保护。<br>[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。                                                                                                                               |
| 5  | Activity (org.cocos2dx.lua.AppActivity) 未被保护。<br>存在一个intent-filter。                                       | 警告   | 发现 Activity与设备上的其他应用程序共享，因此它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。                                                                                                    |
| 6  | Activity (com.jooyuu.fusionsdk.SDKLaunchActivity) 未被保护。<br>存在一个intent-filter。                             | 警告   | 发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。                                                                                                   |
| 7  | Activity (com.jooyuu.fusionsdk.util.privacy.FusionPrivacyActivitySingle) 未被保护。<br>[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。                                                                                                                                         |
| 8  | Activity (com.jooyuu.fusionsdk.util.privacy.FusionPrivacyActivity) 未被保护。<br>[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。                                                                                                                                         |
| 9  | Activity (com.jooyuu.fusionsdk.util.privacy.FusionPrivacyActivity2) 未被保护。<br>[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。                                                                                                                                         |
| 10 | Activity (w1.MainActivity) 未被保护。<br>[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。                                                                                                                                         |
| 11 | Activity (view.TestLoginActivity) 未被保护。<br>[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。                                                                                                                                         |
| 12 | Content Provider (com.vivo.union.sdk.VivoUnionProvider) 未被保护。<br>[android:exported=true]                  | 警告   | 发现 Content Provider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。                                                                                                                                 |

代码安全漏洞检测

高危: 4 | 警告: 9 | 信息: 2 | 安全: 2 | 屏蔽: 0

| 序号 | 问题                                                                                   | 等级 | 参考标准                                                                                                          | 文件位置                         |
|----|--------------------------------------------------------------------------------------|----|---------------------------------------------------------------------------------------------------------------|------------------------------|
| 1  | <a href="#">应用程序记录日志信息,不得记录敏感信息</a>                                                  | 信息 | CWE: CWE-532: 通过日志文件的信息暴露<br>OWASP MASVS: MSTG-STORAGE-3                                                      | <a href="#">升级会员: 解锁高级权限</a> |
| 2  | <a href="#">MD5是已知存在哈希冲突的弱哈希</a>                                                     | 警告 | CWE: CWE-327: 使用了破损或被认为是不安全的加密算法<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | <a href="#">升级会员: 解锁高级权限</a> |
| 3  | <a href="#">文件可能包含硬编码的敏感信息,如用户名、密码、密钥等</a>                                           | 警告 | CWE: CWE-312: 明文存储敏感信息<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14               | <a href="#">升级会员: 解锁高级权限</a> |
| 4  | IP地址泄露                                                                               | 警告 | CWE: CWE-200: 信息泄露<br>OWASP MASVS: MSTG-CODE-2                                                                | <a href="#">升级会员: 解锁高级权限</a> |
| 5  | <a href="#">SHA-1是已知存在哈希冲突的弱哈希</a>                                                   | 警告 | CWE: CWE-327: 使用了破损或被认为是不安全的加密算法<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | <a href="#">升级会员: 解锁高级权限</a> |
| 6  | <a href="#">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</a>                               | 警告 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2               | <a href="#">升级会员: 解锁高级权限</a> |
| 7  | <a href="#">应用程序可能具有Rootkit功能</a>                                                    | 安全 | OWASP MASVS: MSTG-RESILIENCE-1                                                                                | <a href="#">升级会员: 解锁高级权限</a> |
| 8  | <a href="#">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</a> | 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')<br>OWASP Top 10: M7: Client Code Quality                           | <a href="#">升级会员: 解锁高级权限</a> |

|    |                                                                                            |    |                                                                                                                        |                             |
|----|--------------------------------------------------------------------------------------------|----|------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| 9  | <a href="#">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。</a>                            | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-3     | <a href="#">升级会员：解锁高级权限</a> |
| 10 | <a href="#">SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击</a>                           | 高危 | CWE: CWE-295: 证书验证不恰当<br>OWASP Top 10: M3: Insecure Communication<br>OWASP MASVS: MSTG-NETWORK-3                       | <a href="#">升级会员：解锁高级权限</a> |
| 11 | <a href="#">不安全的Web视图实现。可能存在WebView任意代码执行漏洞</a>                                            | 警告 | CWE: CWE-749: 暴露危险方法或函数<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7                   | <a href="#">升级会员：解锁高级权限</a> |
| 12 | <a href="#">不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击</a>                         | 高危 | CWE: CWE-295: 证书验证不恰当<br>OWASP Top 10: M3: Insecure Communication<br>OWASP MASVS: MSTG-NETWORK-3                       | <a href="#">升级会员：解锁高级权限</a> |
| 13 | <a href="#">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</a>                                    | 安全 | OWASP MASVS: MSTG-NETWORK-4                                                                                            | <a href="#">升级会员：解锁高级权限</a> |
| 14 | <a href="#">可能存在跨域漏洞。在WebView中启用从URL访问文件可能会泄漏文件系统中的敏感信息</a>                                | 警告 | CWE: CWE-200: 信息泄露<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7                        | <a href="#">升级会员：解锁高级权限</a> |
| 15 | <a href="#">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</a> | 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'）<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-6 | <a href="#">升级会员：解锁高级权限</a> |

|    |                                                           |    |                                                                                                      |                             |
|----|-----------------------------------------------------------|----|------------------------------------------------------------------------------------------------------|-----------------------------|
| 16 | <a href="#">应用程序使用不安全的随机数生成器</a>                          | 警告 | CWE: CWE-330: 使用不充分的随机数<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | <a href="#">升级会员：解锁高级权限</a> |
| 17 | <a href="#">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</a> | 信息 | OWASP MASVS: MSTG-STORAGE-10                                                                         | <a href="#">升级会员：解锁高级权限</a> |

🚩 Native 库安全加固检测

|    |     |            |     |                    |       |                  |                    |                   |                          |
|----|-----|------------|-----|--------------------|-------|------------------|--------------------|-------------------|--------------------------|
| 序号 | 动态库 | NX(堆栈禁止执行) | PIE | STACK CANNARY(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) |
|----|-----|------------|-----|--------------------|-------|------------------|--------------------|-------------------|--------------------------|

|   |                             |                                                                             |                                                                                                |                                                                                                 |                                                                                                                          |                                                              |                                                        |                                                                                                                                                     |                                   |
|---|-----------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| 1 | arm64-v8a/libCtaApiWYLib.so | <p>True<br/>info</p> <p>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。</p> | <p>动态共享对象 (DSO)<br/>info</p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p> | <p>True<br/>info</p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。</p> | <p>Full RELRO<br/>info</p> <p>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。</p> | <p>No<br/>ne<br/>info</p> <p>二进制文件没有设置运行时搜索路径或RPATH</p>      | <p>No<br/>n<br/>e<br/>info</p> <p>二进制文件没有设置RUNPATH</p> | <p>False<br/>warning</p> <p>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。</p> | <p>True<br/>info</p> <p>符号被剥离</p> |
| 2 | arm64-v8a/libEncryptorP.so  | <p>True<br/>info</p> <p>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。</p> | <p>动态共享对象 (DSO)<br/>info</p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p> | <p>True<br/>info</p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。</p> | <p>Full RELRO<br/>info</p> <p>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。</p> | <p>No<br/>n<br/>e<br/>info</p> <p>二进制文件没有设置运行时搜索路径或RPATH</p> | <p>No<br/>n<br/>e<br/>info</p> <p>二进制文件没有设置RUNPATH</p> | <p>False<br/>warning</p> <p>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。</p> | <p>True<br/>info</p> <p>符号被剥离</p> |

|   |                          |                                                                             |                                                                                                |                                                                                                 |                                                                                                                          |                                                                   |                                                                  |                                                                                                                                                                                                                 |                                                  |
|---|--------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| 3 | arm64-v8a/libgism.so     | <p>True<br/>info</p> <p>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。</p> | <p>动态共享对象(DSO)</p> <p>info</p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。</p> | <p>True<br/>info</p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。</p> | <p>Full RELRO<br/>info</p> <p>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。</p> | <p>No<br/>ne<br/>inf<br/>o</p> <p>二进制文件没有设置运行时搜索路径或RPATH</p>      | <p>N<br/>o<br/>n<br/>e<br/>in<br/>fo</p> <p>二进制文件没有设置RUNPATH</p> | <p>False<br/>warning</p> <p>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。</p>                                                              | <p>Tr<br/>u<br/>e<br/>in<br/>fo</p> <p>符号被剥离</p> |
| 4 | arm64-v8a/liblayaaair.so | <p>True<br/>info</p> <p>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。</p> | <p>动态共享对象(DSO)</p> <p>info</p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。</p> | <p>True<br/>info</p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。</p> | <p>Full RELRO<br/>info</p> <p>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。</p> | <p>No<br/>n<br/>e<br/>in<br/>fo</p> <p>二进制文件没有设置运行时搜索路径或RPATH</p> | <p>N<br/>o<br/>n<br/>e<br/>in<br/>fo</p> <p>二进制文件没有设置RUNPATH</p> | <p>True<br/>info</p> <p>二进制文件有以下加固函数: ['__strlen_chk', '__memcpy_chk', '__memset_chk', '__vsnprintf_chk', '__strcat_chk', '__memmove_chk', '__vsprintf_chk', '__fgets_chk', '__strcpy_chk', '__strchr_chk']</p> | <p>Tr<br/>u<br/>e<br/>in<br/>fo</p> <p>符号被剥离</p> |

|   |                         |                                                                                             |                                                                                                             |                                                                                                                 |                                                                                                                                          |                                                                     |                                                               |                                                                                                                                 |                                                   |
|---|-------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| 5 | arm64-v8a/libluster.so  | <p>True<br/><a href="#">info</a></p> <p>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。</p> | <p>动态共享对象(DSO)<br/><a href="#">info</a></p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。</p> | <p>True<br/><a href="#">info</a></p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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。</p> | <p>No<br/><a href="#">ne info</a></p> <p>二进制文件没有设置运行时搜索路径或RPATH</p> | <p>No<br/><a href="#">ne info</a></p> <p>二进制文件没有设置RUNPATH</p> | <p>True<br/><a href="#">info</a></p> <p>二进制文件有以下加固函数: ['__strlen_chk', '__strncpy_chk', '__strcpy_chk']</p>                     | <p>True<br/><a href="#">info</a></p> <p>符号被剥离</p> |
| 6 | arm64-v8a/libterrain.so | <p>True<br/><a href="#">info</a></p> <p>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。</p> | <p>动态共享对象(DSO)<br/><a href="#">info</a></p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。</p> | <p>True<br/><a href="#">info</a></p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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。</p> | <p>No<br/><a href="#">ne info</a></p> <p>二进制文件没有设置运行时搜索路径或RPATH</p> | <p>No<br/><a href="#">ne info</a></p> <p>二进制文件没有设置RUNPATH</p> | <p>True<br/><a href="#">info</a></p> <p>二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__vsprintf_chk']</p> | <p>True<br/><a href="#">info</a></p> <p>符号被剥离</p> |

|   |                          |                                                                                             |                                                                                                             |                                                                                                                 |                                                                                                                                          |                                                                         |                                                                                    |                                                                                                                                                                     |                                                   |
|---|--------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| 7 | arm64-v8a/libturingad.so | <p>True<br/><a href="#">info</a></p> <p>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。</p> | <p>动态共享对象(DSO)<br/><a href="#">info</a></p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程(ROP)攻击更难可靠地执行。</p> | <p>True<br/><a href="#">info</a></p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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。</p> | <p>No<br/><a href="#">ne<br/>info</a></p> <p>二进制文件没有设置运行时搜索路径或RPATH</p> | <p>No<br/><a href="#">n<br/>o<br/>n<br/>e<br/>info</a></p> <p>二进制文件没有设置RUNPATH</p> | <p>False<br/><a href="#">warning</a></p> <p>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。</p> | <p>True<br/><a href="#">info</a></p> <p>符号被剥离</p> |
|---|--------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|

应用行为分析

| 编号    | 行为                            | 标签           | 文件                          |
|-------|-------------------------------|--------------|-----------------------------|
| 00096 | 连接到 URL 并设置请求方法               | 命令<br>网络     | <a href="#">升级会员：解锁高级权限</a> |
| 00089 | 连接到 URL 并接收来自服务器的输入流          | 命令<br>网络     | <a href="#">升级会员：解锁高级权限</a> |
| 00109 | 连接到 URL 并获取响应代码               | 网络<br>命令     | <a href="#">升级会员：解锁高级权限</a> |
| 00094 | 连接到 URL 并从内读取数据               | 命令<br>网络     | <a href="#">升级会员：解锁高级权限</a> |
| 00108 | 从给定的 URL 读取输入流                | 网络<br>命令     | <a href="#">升级会员：解锁高级权限</a> |
| 00063 | 拨打电话（查看网页、拨打电话等）              | 控制           | <a href="#">升级会员：解锁高级权限</a> |
| 00051 | 通过setData隐式意图（查看网页、拨打电话等）     | 控制           | <a href="#">升级会员：解锁高级权限</a> |
| 00036 | 从 res/raw 目录获取资源文件            | 反射           | <a href="#">升级会员：解锁高级权限</a> |
| 00053 | 监视给定内容 URI 标识的数据更改（SMS、MMS 等） | 短信           | <a href="#">升级会员：解锁高级权限</a> |
| 00038 | 查询电话号码                        | 信息收集         | <a href="#">升级会员：解锁高级权限</a> |
| 00130 | 获取当前WIFI信息                    | WiFi<br>信息收集 | <a href="#">升级会员：解锁高级权限</a> |
| 00033 | 查询IMEI号                       | 信息收集         | <a href="#">升级会员：解锁高级权限</a> |

|       |                        |              |                             |
|-------|------------------------|--------------|-----------------------------|
| 00083 | 查询IMEI号                | 信息收集<br>电话服务 | <a href="#">升级会员：解锁高级权限</a> |
| 00009 | 将游标中的数据放入JSON对象        | 文件           | <a href="#">升级会员：解锁高级权限</a> |
| 00191 | 获取短信收件箱中的消息            | 短信           | <a href="#">升级会员：解锁高级权限</a> |
| 00121 | 创建目录                   | 文件<br>命令     | <a href="#">升级会员：解锁高级权限</a> |
| 00125 | 检查给定的文件路径是否存在          | 文件           | <a href="#">升级会员：解锁高级权限</a> |
| 00104 | 检查给定路径是否是目录            | 文件           | <a href="#">升级会员：解锁高级权限</a> |
| 00030 | 通过给定的 URL 连接到远程服务器     | 网络           | <a href="#">升级会员：解锁高级权限</a> |
| 00067 | 查询IMSI号码               | 信息收集         | <a href="#">升级会员：解锁高级权限</a> |
| 00022 | 从给定的文件绝对路径打开文件         | 文件           | <a href="#">升级会员：解锁高级权限</a> |
| 00013 | 读取文件并将其放入流中            | 文件           | <a href="#">升级会员：解锁高级权限</a> |
| 00062 | 查询WiFi信息和WiFi Mac地址    | WiFi<br>信息收集 | <a href="#">升级会员：解锁高级权限</a> |
| 00082 | 获取当前WiFi MAC地址         | 信息收集<br>WiFi | <a href="#">升级会员：解锁高级权限</a> |
| 00014 | 将文件读入流并将其放入 JSON 对象中   | 文件           | <a href="#">升级会员：解锁高级权限</a> |
| 00005 | 获取文件的绝对路径并将其放入 JSON 对象 | 文件           | <a href="#">升级会员：解锁高级权限</a> |
| 00054 | 从文件安装其他APK             | 反射           | <a href="#">升级会员：解锁高级权限</a> |
| 00072 | 将 HTTP 输入流写入文件         | 网络<br>文件     | <a href="#">升级会员：解锁高级权限</a> |
| 00015 | 将缓冲流（数据）放入 JSON 对象     | 文件           | <a href="#">升级会员：解锁高级权限</a> |
| 00012 | 读取数据并放入缓冲流             | 文件           | <a href="#">升级会员：解锁高级权限</a> |
| 00202 | 打电话                    | 控制           | <a href="#">升级会员：解锁高级权限</a> |
| 00203 | 将电话号码放入意图中             | 控制           | <a href="#">升级会员：解锁高级权限</a> |
| 00123 | 连接到远程服务器后将响应保存为 JSON   | 网络<br>命令     | <a href="#">升级会员：解锁高级权限</a> |
| 00134 | 获取当前WiFi IP地址          | WiFi<br>信息收集 | <a href="#">升级会员：解锁高级权限</a> |
| 00091 | 从广播中检索数据               | 信息收集         | <a href="#">升级会员：解锁高级权限</a> |

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.GET_TASKS<br>android.permission.READ_PHONE_STATE<br>android.permission.RECEIVE_BOOT_COMPLETED<br>android.permission.SYSTEM_ALERT_WINDOW<br>android.permission.MODIFY_AUDIO_SETTINGS<br>android.permission.REQUEST_INSTALL_PACKAGES                                                                          |
| 其它常用权限   | 8/46 | android.permission.INTERNET<br>android.permission.REORDER_TASKS<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.CHANGE_NETWORK_STATE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.CHANGE_WIFI_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。

🔍 恶意域名威胁检测

| 域名                        | 状态 | 中国境内 | 位置信息                                                                                                              |
|---------------------------|----|------|-------------------------------------------------------------------------------------------------------------------|
| joint.vivo.com.cn         | 安全 | 是    | IP地址: 47.98.200.126<br>国家: 中国<br>地区: 江西<br>城市: 九江<br>纬度: 29.733330<br>经度: 115.983330<br>查看: <a href="#">高德地图</a>  |
| joint-account.vivo.com.cn | 安全 | 是    | IP地址: 47.98.200.126<br>国家: 中国<br>地区: 浙江<br>城市: 杭州<br>纬度: 30.293650<br>经度: 120.161583<br>查看: <a href="#">高德地图</a>  |
| st-onlinegame.vivo.com.cn | 安全 | 是    | IP地址: 47.98.200.126<br>国家: 中国<br>地区: 北京<br>城市: 北京<br>纬度: 39.907501<br>经度: 116.397102<br>查看: <a href="#">高德地图</a>  |
| pay.vivo.com.cn           | 安全 | 是    | IP地址: 47.98.200.126<br>国家: 中国<br>地区: 江苏<br>城市: 连云港<br>纬度: 34.600025<br>经度: 119.166847<br>查看: <a href="#">高德地图</a> |

|                     |    |   |                                                                                                                                                                              |
|---------------------|----|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| overseasdk.98wan.cn | 安全 | 是 | <b>IP地址:</b> 119.91.58.41<br><b>国家:</b> 中国<br><b>地区:</b> 广东<br><b>城市:</b> 广州<br><b>纬度:</b> 23.127361<br><b>经度:</b> 113.264572<br><b>查看:</b> <a href="#">高德地图</a>             |
| fssdk.98wan.cn      | 安全 | 是 | <b>IP地址:</b> 119.91.58.41<br><b>国家:</b> 中国<br><b>地区:</b> 广东<br><b>城市:</b> 广州<br><b>纬度:</b> 23.127361<br><b>经度:</b> 113.264572<br><b>查看:</b> <a href="#">高德地图</a>             |
| api.mengxuanwl.com  | 安全 | 是 | <b>IP地址:</b> 47.98.200.126<br><b>国家:</b> 中国<br><b>地区:</b> 浙江<br><b>城市:</b> 杭州<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161583<br><b>查看:</b> <a href="#">高德地图</a>            |
| www.xxx.com         | 安全 | 否 | <b>IP地址:</b> 41.0.173.173<br><b>国家:</b> 荷兰(王国)<br><b>地区:</b> 北荷兰省<br><b>城市:</b> 阿姆斯特丹<br><b>纬度:</b> 52.378502<br><b>经度:</b> 4.899980<br><b>查看:</b> <a href="#">Google 地图</a> |
| sdk2.98wan.cn       | 安全 | 是 | <b>IP地址:</b> 106.52.86.240<br><b>国家:</b> 中国<br><b>地区:</b> 广东<br><b>城市:</b> 广州<br><b>纬度:</b> 23.127361<br><b>经度:</b> 113.264572<br><b>查看:</b> <a href="#">高德地图</a>            |
| crbug.com           | 安全 | 否 | <b>IP地址:</b> 216.239.32.29<br><b>国家:</b> 美国<br><b>地区:</b> 加利福尼亚<br><b>城市:</b> 山景城<br><b>纬度:</b> 37.405991<br><b>经度:</b> -122.078514<br><b>查看:</b> <a href="#">Google 地图</a>  |
| topic.vivo.com.cn   | 安全 | 是 | <b>IP地址:</b> 47.98.200.126<br><b>国家:</b> 中国<br><b>地区:</b> 江苏<br><b>城市:</b> 苏州<br><b>纬度:</b> 31.311365<br><b>经度:</b> 120.617691<br><b>查看:</b> <a href="#">高德地图</a>            |

|                            |    |   |                                                                                                                                                                                |
|----------------------------|----|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| usrsysjoint.vivo.com.cn    | 安全 | 是 | <b>IP地址:</b> 47.98.200.126<br><b>国家:</b> 中国<br><b>地区:</b> 北京<br><b>城市:</b> 北京<br><b>纬度:</b> 39.907501<br><b>经度:</b> 116.397102<br><b>查看:</b> <a href="#">高德地图</a>              |
| docs.sentry.io             | 安全 | 否 | <b>IP地址:</b> 141.0.173.173<br><b>国家:</b> 美国<br><b>地区:</b> 加利福尼亚<br><b>城市:</b> 核桃<br><b>纬度:</b> 34.015400<br><b>经度:</b> -117.858200<br><b>查看:</b> <a href="#">Google 地图</a>     |
| xxx.com                    | 安全 | 否 | <b>IP地址:</b> 141.0.173.173<br><b>国家:</b> 荷兰 (王国)<br><b>地区:</b> 北荷兰省<br><b>城市:</b> 阿姆斯特丹<br><b>纬度:</b> 52.378502<br><b>经度:</b> 4.899980<br><b>查看:</b> <a href="#">Google 地图</a> |
| senlogs.kkyou.cn           | 安全 | 是 | <b>IP地址:</b> 141.0.173.100<br><b>国家:</b> 中国<br><b>地区:</b> 广东<br><b>城市:</b> 广州<br><b>纬度:</b> 23.127361<br><b>经度:</b> 113.264572<br><b>查看:</b> <a href="#">高德地图</a>              |
| sdk.98wan.cn               | 安全 | 是 | <b>IP地址:</b> 106.52.86.240<br><b>国家:</b> 中国<br><b>地区:</b> 广东<br><b>城市:</b> 广州<br><b>纬度:</b> 23.127361<br><b>经度:</b> 113.264572<br><b>查看:</b> <a href="#">高德地图</a>              |
| overseafssdk.98wan.cn      | 安全 | 是 | <b>IP地址:</b> 43.159.198.36<br><b>国家:</b> 中国<br><b>地区:</b> 香港<br><b>城市:</b> 香港<br><b>纬度:</b> 22.285521<br><b>经度:</b> 114.157692<br><b>查看:</b> <a href="#">高德地图</a>              |
| st-offlinegame.vivo.com.cn | 安全 | 是 | <b>IP地址:</b> 220.181.128.250<br><b>国家:</b> 中国<br><b>地区:</b> 北京<br><b>城市:</b> 北京<br><b>纬度:</b> 39.907501<br><b>经度:</b> 116.397102<br><b>查看:</b> <a href="#">高德地图</a>            |

|                         |    |   |                                                                                                                                                                     |
|-------------------------|----|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| btfssdk.98wan.cn        | 安全 | 是 | <b>IP地址:</b> 106.52.86.240<br><b>国家:</b> 中国<br><b>地区:</b> 浙江<br><b>城市:</b> 温州<br><b>纬度:</b> 27.999420<br><b>经度:</b> 120.666817<br><b>查看:</b> <a href="#">高德地图</a>   |
| appdetailh5.vivo.com.cn | 安全 | 是 | <b>IP地址:</b> 61.160.238.63<br><b>国家:</b> 中国<br><b>地区:</b> 江苏<br><b>城市:</b> 常州<br><b>纬度:</b> 31.783331<br><b>经度:</b> 119.966666<br><b>查看:</b> <a href="#">高德地图</a>   |
| h5frontend.ddtugame.com | 安全 | 是 | <b>IP地址:</b> 182.182.215.115<br><b>国家:</b> 中国<br><b>地区:</b> 江苏<br><b>城市:</b> 徐州<br><b>纬度:</b> 34.266666<br><b>经度:</b> 117.166664<br><b>查看:</b> <a href="#">高德地图</a> |

🌐 URL 链接安全分析

| URL信息                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 源码文件                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <ul style="list-style-type: none"><li>http://bsycdn.kkyou.cn/w6/qudaoceshi/android/current/bin/</li><li>https://daily.m.zzx9.cn</li><li>http://bsycdn.kkyou.cn/w6d/versions/0.3.1/newest/bin</li><li>http://engine.layabox.com/layaAppUpdate/layaApp/v2.1/</li><li>http://stand.alone.version</li><li>http://bsycdn.kkyou.cn/w6d/versions/0.3.1/newest/bin/apprelease.html</li><li>http://central.w6d.kkyou.cn/api/</li><li>http://runtime.layabox.com/font/simhei.ttf</li><li>http://www.9377.com/</li><li>http://nativetest.layabox.com/laya/laya-2.0.1/index.js</li><li>https://api.mengxuanwl.com/Api/PayBack/VerBack/ver/mxsdk_xkfb_vivo/vm/vivo/appid/658</li><li>https://auth.wosms.cn</li><li>http://bsycdn.kkyou.cn/w6/qudaoceshi/android/current/bin/apprelease.html?platname=qudaoces</li><li>hi&amp;v=6</li><li>http://w6d.kkyou.cn/xiaoyu_xiaoyu_xkfb/android/version.php</li><li>http://stand.alone.version/index.js</li></ul> | 自研引擎-A                                                   |
| <ul style="list-style-type: none"><li>https://pay.vivo.com.cn/vcoin/wap/cashier/</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | com/vivo/unionsdk/n/a.java                               |
| <ul style="list-style-type: none"><li>https://docs.sentry.io/clients/java/modules/android/</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | io/sentry/android/AndroidSentryClientFa<br>ctory.java    |
| <ul style="list-style-type: none"><li>https://joint.vivo.com.cn/ops/getattributioninfo</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | com/vivounion/ic/channelreader/NetCha<br>nnelReader.java |
| <ul style="list-style-type: none"><li>https://pay.vivo.com.cn</li><li>https://joint.vivo.com.cn</li><li>https://jointaccount.vivo.com.cn</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | com/vivo/unionsdk/g.java                                 |
| <ul style="list-style-type: none"><li>4.7.7.1</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | com/vivo/unionsdk/utils/Helpers.java                     |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| <ul style="list-style-type: none"> <li>• <a href="http://7847ff45c3294417b1257fe81028557e@senlogs.kkyou.cn/13">http://7847ff45c3294417b1257fe81028557e@senlogs.kkyou.cn/13</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | w1/SentryUtils.java                           |
| <ul style="list-style-type: none"> <li>• <a href="https://joint.vivo.com.cn/game-subaccount-login">https://joint.vivo.com.cn/game-subaccount-login</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | com/vivo/sdkplugin/a.java                     |
| <ul style="list-style-type: none"> <li>• <a href="http://www.xxx.com/xxx.jpg">http://www.xxx.com/xxx.jpg</a></li> <li>• <a href="http://xxx.com/xxx.jpg">http://xxx.com/xxx.jpg</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | w1/RuntimeProxy.java                          |
| <ul style="list-style-type: none"> <li>• 4.7.7.1</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | com/vivo/unionsdk/m/b/a.java                  |
| <ul style="list-style-type: none"> <li>• 4.7.7.1</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | com/vivo/unionsdk/p/g.java                    |
| <ul style="list-style-type: none"> <li>• <a href="http://overseafssdk.98wan.cn/">http://overseafssdk.98wan.cn/</a></li> <li>• <a href="http://overseasdk.98wan.cn/">http://overseasdk.98wan.cn/</a></li> <li>• <a href="http://fssdk.98wan.cn/">http://fssdk.98wan.cn/</a></li> <li>• <a href="http://sdk2.98wan.cn/">http://sdk2.98wan.cn/</a></li> <li>• <a href="http://btfssdk.98wan.cn/">http://btfssdk.98wan.cn/</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                 | com/jooyuu/fusionsdk/constant/JyMiYue.java    |
| <ul style="list-style-type: none"> <li>• <a href="http://sdk2.98wan.cn/api/guest.do">http://sdk2.98wan.cn/api/guest.do</a></li> <li>• <a href="http://sdk2.98wan.cn/api/modifyaccount.do">http://sdk2.98wan.cn/api/modifyaccount.do</a></li> <li>• <a href="http://sdk2.98wan.cn/api/login.do">http://sdk2.98wan.cn/api/login.do</a></li> <li>• <a href="http://sdk2.98wan.cn/api/cardverify.do">http://sdk2.98wan.cn/api/cardverify.do</a></li> <li>• <a href="http://sdk2.98wan.cn/api/sendverifycode.do">http://sdk2.98wan.cn/api/sendverifycode.do</a></li> <li>• <a href="http://sdk2.98wan.cn/api/help.do?fs_app_id=%s&amp;game_id=%s">http://sdk2.98wan.cn/api/help.do?fs_app_id=%s&amp;game_id=%s</a></li> <li>• <a href="http://sdk.98wan.cn/api/sdk/android_sdkconfig.php">http://sdk.98wan.cn/api/sdk/android_sdkconfig.php</a></li> </ul> | com/jooyuu/fusionsdk/constant/JyConstant.java |
| <ul style="list-style-type: none"> <li>• <a href="https://joint.vivo.com.cn/game-subaccount-login">https://joint.vivo.com.cn/game-subaccount-login</a></li> <li>• <a href="https://usrsysjoint.vivo.com.cn/realnameauth/isauthed">https://usrsysjoint.vivo.com.cn/realnameauth/isauthed</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | com/vivo/unionsdk/m/a/c.java                  |
| <ul style="list-style-type: none"> <li>• <a href="https://docs.sentry.io/clients/java/config/#in-application-stack-frames">https://docs.sentry.io/clients/java/config/#in-application-stack-frames</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | io/sentry/DefaultSentryClientFactory.java     |
| <ul style="list-style-type: none"> <li>• <a href="https://joint.vivo.com.cn/base/sdkupdatecheck">https://joint.vivo.com.cn/base/sdkupdatecheck</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | com/vivo/unionsdk/m/d/c/c/a.java              |
| <ul style="list-style-type: none"> <li>• <a href="https://h5frontend.ddtugame.com/platform/sdk_pf/1.0.0/popup_window/index.html#?appid=">https://h5frontend.ddtugame.com/platform/sdk_pf/1.0.0/popup_window/index.html#?appid=</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | com/mxsdk/view/Djqdialog.java                 |
| <ul style="list-style-type: none"> <li>• 4.7.7.1</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | com/vivo/unionsdk/m/a/a.java                  |
| <ul style="list-style-type: none"> <li>• <a href="https://joint.vivo.com.cn/ops/allowchannelinfo">https://joint.vivo.com.cn/ops/allowchannelinfo</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | com/vivo/unionsdk/k/d.java                    |
| <ul style="list-style-type: none"> <li>• 4.7.7.1</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | com/vivo/unionsdk/t/b.java                    |
| <ul style="list-style-type: none"> <li>• <a href="http://dp3.qq.com/stdlog">http://dp3.qq.com/stdlog</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | com/qq/gdt/action/f/a.java                    |
| <ul style="list-style-type: none"> <li>• javascript&gt;window.conchback&amp;&amp;window.conchback</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | layaaair/game/browser/bf.java                 |
| <ul style="list-style-type: none"> <li>• <a href="https://docs.sentry.io/clients/java/config/">https://docs.sentry.io/clients/java/config/</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | io/sentry/event/EventBuilder.java             |
| <ul style="list-style-type: none"> <li>• <a href="https://topic.vivo.com.cn/joint/tp33em3gb3bi0/index.html">https://topic.vivo.com.cn/joint/tp33em3gb3bi0/index.html</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | com/vivo/sdkplugin/k/b.java                   |
| <ul style="list-style-type: none"> <li>• <a href="https://api.mengxuanwl.com">https://api.mengxuanwl.com</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | com/mxsdk/constants/Constants.java            |
| <ul style="list-style-type: none"> <li>• 4.7.7.1</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | com/vivo/unionsdk/dynamic/stability/a.java    |
| <ul style="list-style-type: none"> <li>• <a href="https://st-onlinegame.vivo.com.cn">https://st-onlinegame.vivo.com.cn</a></li> <li>• <a href="https://st-offlinegame.vivo.com.cn">https://st-offlinegame.vivo.com.cn</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | com/vivo/unionsdk/t/a.java                    |
| <ul style="list-style-type: none"> <li>• <a href="https://docs.sentry.io/clients/java/">https://docs.sentry.io/clients/java/</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | io/sentry/dsn/Dsn.java                        |
| <ul style="list-style-type: none"> <li>• <a href="https://api.mengxuanwl.com/home/index/index/mxyh.html">https://api.mengxuanwl.com/home/index/index/mxyh.html</a></li> <li>• <a href="https://api.mengxuanwl.com/home/index/index/mxys.html">https://api.mengxuanwl.com/home/index/index/mxys.html</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | com/mxsdk/ui/dialog/KLCommonDialog.java       |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| <ul style="list-style-type: none"><li>https://appdetailh5.vivo.com.cn/detail/1873310</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | com/vivo/unionsdk/cmd/JumpUtils.java             |
| <ul style="list-style-type: none"><li>4.7.7.1</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | com/vivo/unionsdk/dynamic/client/internal/a.java |
| <ul style="list-style-type: none"><li>http://a.gdt.qq.com/sdk</li><li>https://a.gdt.qq.com/sdk</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | com/qq/gdt/action/f/c.java                       |
| <ul style="list-style-type: none"><li>4.7.7.1</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | com/vivo/unionsdk/VivoUnionProvider.java         |
| <ul style="list-style-type: none"><li>http://a.gdt.qq.com/getsdkconf</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | com/qq/gdt/action/f/b.java                       |
| <ul style="list-style-type: none"><li>javascript:document.body.innerHTML=</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | com/vivo/unionsdk/u/d.java                       |
| <ul style="list-style-type: none"><li>https://h5frontend.ddtugame.com/platform/sdk_pf/1.0.0/popup_window/index.html#/?appid=</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | com/mx/sdk/window/Popupdialog.java               |
| <ul style="list-style-type: none"><li>data::serializecallcode</li><li>data::serializerecursiveasboilerplate</li><li>data::serializebackpointer</li><li>ftp://%s:%s@%s</li><li>data::kmagicnumber</li><li>1.2.0.4</li><li>data::serializeowndescriptors</li><li>data::serializeprototype</li><li>data::serializeelementskindgeneralizations</li><li>data::serializeasregexpboilerplate</li><li>data::serializecontents</li><li>data::serializeobjectcreatemap</li><li>file://hostname/</li><li>data::stack_is_iterable_address</li><li>data::serializeboilerplate</li><li>data::serializeconstructor</li><li>data::klastdeoptimizekind</li><li>data::fast_c_call_caller_pc_address</li><li>data::serializeforelementload</li><li>https://crbug.com/v8/8520</li><li>data::serializeforelementstore</li><li>127.0.0.1</li><li>data::fast_c_call_caller_fp_address</li><li>data::serializeowndescriptor</li><li>data::serializeelements</li><li>data::serializeroommap</li></ul> | lib/arm64-v8a/liblayaaair.so                     |

第三方 SDK 组件分析

| SDK名称   | 开发者                     | 描述信息                                                                                                    |
|---------|-------------------------|---------------------------------------------------------------------------------------------------------|
| MSA SDK | <a href="#">移动安全联盟</a>  | 移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。                                   |
| Bugly   | <a href="#">Tencent</a> | 腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。                                       |
| C++ 共享库 | <a href="#">Android</a> | 在 Android 应用中运行原生代码。                                                                                    |
| LayaAir | <a href="#">Layabox</a> | LayaAir 是一个开源的 2D/3D 引擎，专为高性能游戏而设计。LayaAir 支持 TypeScript、JavaScript 和 ActionScript 3.0 编程语言。一次开发，多平台发布。 |

|               |                            |                                                                                            |
|---------------|----------------------------|--------------------------------------------------------------------------------------------|
| vivo 网游联运 SDK | <a href="#">vivo</a>       | 使用 vivo 账号统一登录，支付，并提供统一的实名认证服务。                                                            |
| DataFinder    | <a href="#">Volcengine</a> | 基于灵活高效的分析模型，发现用户行为数据的价值，进而转化为促进增长的行动。                                                      |
| File Provider | <a href="#">Android</a>    | 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 Media | <a href="#">Google</a>     | 与其他应用共享媒体内容和控件。已被 media2 取代。                                                               |

✉ 邮箱地址敏感信息提取

| EMAIL                                             | 源码文件                |
|---------------------------------------------------|---------------------|
| 7847ff45c3294417b1257fe81028557e@senlogs.kkyou.cn | w1/SentryUtils.java |

🕒 第三方追踪器检测

| 名称     | 类别              | 网址                                                                                                                  |
|--------|-----------------|---------------------------------------------------------------------------------------------------------------------|
| Bugly  |                 | <a href="https://reports.exodus-privacy.eu.org/trackers/190">https://reports.exodus-privacy.eu.org/trackers/190</a> |
| Pangle | Advertisement   | <a href="https://reports.exodus-privacy.eu.org/trackers/363">https://reports.exodus-privacy.eu.org/trackers/363</a> |
| Sentry | Crash reporting | <a href="https://reports.exodus-privacy.eu.org/trackers/412">https://reports.exodus-privacy.eu.org/trackers/412</a> |

🔑 敏感凭证泄露检测

|                                                                    |
|--------------------------------------------------------------------|
| 可能的密钥                                                              |
| 凭证信息=> "vivoUnionAppId" : "105873260"                              |
| "umcsdk_oauth_version_name" : "v1.4.1"                             |
| 7847ff45c3294417b1257fe81028557e                                   |
| MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDIxHA9yA16YbRRJqi+UB5jhbb    |
| D18650CDE78C0CE66F1C21AF75DEE8C7772D4B8BB50289FA58A76E8F68EED2A9E  |
| npD6CFRnTn1D1Wpwr-H4tNkF5yB1TwAUJbI-NsSc7hi4YpttiZISqEnl8UIX+9OWOi |

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