目录

[1. App安全测评总览](#_Toc1780391)

[1.1. App测评得分](#_Toc1780392)

[1.2. App基本信息](#_Toc1780393)

[1.3. App安全测评结果总结](#_Toc1780394)

[2. App安全测评结果详情](#_Toc1780395)

[2.1. 自身安全](#_Toc1780396)

[2.1.1. 权限信息](#_Toc1780397)

[2.1.2. 行为信息](#_Toc1780398)

[2.1.3. 病毒扫描](#_Toc1780399)

[2.1.4. 敏感词信息](#_Toc17803910)

[2.1.5. 第三方SDK检测](#_Toc17803911)

[2.1.6. 资源文件中的Apk文件](#_Toc17803912)

[2.2. 程序源文件安全](#_Toc17803913)

[2.2.1. 加固壳识别](#_Toc17803914)

[2.2.2. Java代码反编译风险](#_Toc17803915)

[2.2.3. So文件破解风险](#_Toc17803916)

[2.2.4. 篡改和二次打包风险](#_Toc17803917)

[2.2.5. Janus签名机制漏洞](#_Toc17803918)

[2.2.6. 资源文件泄露风险](#_Toc17803919)

[2.2.7. 应用签名未校验风险](#_Toc17803920)

[2.2.8. 代码未混淆风险](#_Toc17803921)

[2.2.9. 使用调试证书发布应用风险](#_Toc17803922)

[2.2.10. 仅使用Java代码风险](#_Toc17803923)

[2.2.11. 启动隐藏服务风险](#_Toc17803924)

[2.2.12. 应用签名算法不安全风险](#_Toc17803925)

[2.3. 本地数据存储安全](#_Toc17803926)

[2.3.1. Webview明文存储密码风险](#_Toc17803927)

[2.3.2. Webview File同源策略绕过漏洞](#_Toc17803928)

[2.3.3. 明文数字证书风险](#_Toc17803929)

[2.3.4. 调试日志函数调用风险](#_Toc17803930)

[2.3.5. 数据库注入漏洞](#_Toc17803931)

[2.3.6. AES/DES加密方法不安全使用漏洞](#_Toc17803932)

[2.3.7. RSA加密算法不安全使用漏洞](#_Toc17803933)

[2.3.8. 密钥硬编码漏洞](#_Toc17803934)

[2.3.9. 动态调试攻击风险](#_Toc17803935)

[2.3.10. Webview远程调试风险](#_Toc17803936)

[2.3.11. 应用数据任意备份风险](#_Toc17803937)

[2.3.12. 敏感函数调用风险](#_Toc17803938)

[2.3.13. 数据库文件任意读写漏洞](#_Toc17803939)

[2.3.14. 全局可读写的内部文件漏洞](#_Toc17803940)

[2.3.15. SharedPreferences数据全局可读写漏洞](#_Toc17803941)

[2.3.16. SharedUserId属性设置漏洞](#_Toc17803942)

[2.3.17. Internal Storage数据全局可读写漏洞](#_Toc17803943)

[2.3.18. getDir数据全局可读写漏洞](#_Toc17803944)

[2.3.19. FFmpeg文件读取漏洞](#_Toc17803945)

[2.3.20. Java层动态调试风险](#_Toc17803946)

[2.3.21. 剪切板敏感信息泄露漏洞](#_Toc17803947)

[2.3.22. 内网测试信息残留漏洞](#_Toc17803948)

[2.3.23. 随机数不安全使用漏洞](#_Toc17803949)

[2.3.24. 代码残留URL信息检测](#_Toc17803950)

[2.3.25. 残留账户密码信息检测](#_Toc17803951)

[2.3.26. 残留手机号信息检测](#_Toc17803952)

[2.4. 通信数据传输安全](#_Toc17803953)

[2.4.1. HTTP传输数据风险](#_Toc17803954)

[2.4.2. HTTPS未校验服务器证书漏洞](#_Toc17803955)

[2.4.3. HTTPS未校验主机名漏洞](#_Toc17803956)

[2.4.4. HTTPS允许任意主机名漏洞](#_Toc17803957)

[2.4.5. Webview绕过证书校验漏洞](#_Toc17803958)

[2.4.6. HTTP报文信息泄漏风险](#_Toc17803959)

[2.5. 身份认证安全](#_Toc17803960)

[2.5.1. 界面劫持风险](#_Toc17803961)

[2.5.2. 输入监听风险](#_Toc17803962)

[2.5.3. 截屏攻击风险](#_Toc17803963)

[2.6. 内部数据交互安全](#_Toc17803964)

[2.6.1. 动态注册Receiver风险](#_Toc17803965)

[2.6.2. Content Provider数据泄露漏洞](#_Toc17803966)

[2.6.3. Activity组件导出风险](#_Toc17803967)

[2.6.4. Service组件导出风险](#_Toc17803968)

[2.6.5. Broadcast Receiver组件导出风险](#_Toc17803969)

[2.6.6. Content Provider组件导出风险](#_Toc17803970)

[2.6.7. 本地端口开放越权漏洞](#_Toc17803971)

[2.6.8. PendingIntent错误使用Intent风险](#_Toc17803972)

[2.6.9. Intent组件隐式调用风险](#_Toc17803973)

[2.6.10. Intent Scheme URL攻击漏洞](#_Toc17803974)

[2.6.11. Fragment注入攻击漏洞](#_Toc17803975)

[2.6.12. 反射调用风险](#_Toc17803976)

[2.7. HTML5安全](#_Toc17803977)

[2.7.1. Web Storage数据泄露风险](#_Toc17803978)

[2.7.2. WebSQL注入漏洞](#_Toc17803979)

[2.7.3. InnerHTML的XSS攻击漏洞](#_Toc17803980)

[2.8. 恶意攻击防范能力](#_Toc17803981)

[2.8.1. “应用克隆”漏洞攻击风险](#_Toc17803982)

[2.8.2. 动态注入攻击风险](#_Toc17803983)

[2.8.3. Webview远程代码执行漏洞](#_Toc17803984)

[2.8.4. 未移除有风险的Webview系统隐藏接口漏洞](#_Toc17803985)

[2.8.5. zip文件解压目录遍历漏洞](#_Toc17803986)

[2.8.6. 下载任意apk漏洞](#_Toc17803987)

[2.8.7. 拒绝服务攻击漏洞](#_Toc17803988)

[2.8.8. 从sdcard加载dex风险](#_Toc17803989)

[2.8.9. 从sdcard加载so风险](#_Toc17803990)

[2.8.10. 未使用编译器堆栈保护技术风险](#_Toc17803991)

[2.8.11. 未使用地址空间随机化技术风险](#_Toc17803992)

[2.8.12. Root设备运行风险](#_Toc17803993)

[2.8.13. 不安全的浏览器调用漏洞](#_Toc17803994)

[3. App安全测评依据](#_Toc17803995)

[附录A：安全漏洞危险等级评定标准](#_Toc17803996)

## App安全测评结果总结

|  |  |  |  |
| --- | --- | --- | --- |
|  | **测评项目** | **危险等级** | **测评结果** |
| 自身安全（6项） | | | |
| 1 | 权限信息 | 低 | 提示信息(发现25处) |
| 2 | 行为信息 | 低 | 提示信息(发现118处) |
| 3 | 病毒扫描 | 高 | 安全 |
| 4 | 敏感词信息 | 低 | 安全 |
| 5 | 第三方SDK检测 | 低 | 提示信息(发现8处) |
| 6 | 资源文件中的Apk文件 | 低 | 安全 |
| 程序源文件安全（12项） | | | |
| 7 | 加固壳识别 | 高 | 存在风险(发现1处) |
| 8 | Java代码反编译风险 | 高 | 存在风险(发现13处) |
| 9 | So文件破解风险 | 低 | 存在风险(发现40处) |
| 10 | 篡改和二次打包风险 | 高 | 未执行 |
| 11 | Janus签名机制漏洞 | 高 | 存在漏洞(发现1处) |
| 12 | 资源文件泄露风险 | 低 | 安全 |
| 13 | 应用签名未校验风险 | 高 | 未执行 |
| 14 | 代码未混淆风险 | 中 | 存在风险(发现1处) |
| 15 | 使用调试证书发布应用风险 | 低 | 安全 |
| 16 | 仅使用Java代码风险 | 低 | 安全 |
| 17 | 启动隐藏服务风险 | 低 | 安全 |
| 18 | 应用签名算法不安全风险 | 低 | 安全 |
| 本地数据存储安全（26项） | | | |
| 19 | Webview明文存储密码风险 | 高 | 存在风险(发现1处) |
| 20 | Webview File同源策略绕过漏洞 | 高 | 存在漏洞(发现1处) |
| 21 | 明文数字证书风险 | 中 | 安全 |
| 22 | 调试日志函数调用风险 | 低 | 存在风险(发现435处) |
| 23 | 数据库注入漏洞 | 高 | 未执行 |
| 24 | AES/DES加密方法不安全使用漏洞 | 低 | 存在漏洞(发现6处) |
| 25 | RSA加密算法不安全使用漏洞 | 中 | 存在漏洞(发现4处) |
| 26 | 密钥硬编码漏洞 | 高 | 安全 |
| 27 | 动态调试攻击风险 | 高 | 未执行 |
| 28 | Webview远程调试风险 | 中 | 存在风险(发现1处) |
| 29 | 应用数据任意备份风险 | 中 | 安全 |
| 30 | 敏感函数调用风险 | 低 | 存在风险(发现15处) |
| 31 | 数据库文件任意读写漏洞 | 中 | 安全 |
| 32 | 全局可读写的内部文件漏洞 | 中 | 安全 |
| 33 | SharedPreferences数据全局可读写漏洞 | 中 | 安全 |
| 34 | SharedUserId属性设置漏洞 | 中 | 安全 |
| 35 | Internal Storage数据全局可读写漏洞 | 中 | 安全 |
| 36 | getDir数据全局可读写漏洞 | 中 | 安全 |
| 37 | FFmpeg文件读取漏洞 | 高 | 安全 |
| 38 | Java层动态调试风险 | 中 | 安全 |
| 39 | 剪切板敏感信息泄露漏洞 | 中 | 安全 |
| 40 | 内网测试信息残留漏洞 | 低 | 存在漏洞(发现2处) |
| 41 | 随机数不安全使用漏洞 | 低 | 存在漏洞(发现4处) |
| 42 | 代码残留URL信息检测 | 低 | 安全 |
| 43 | 残留账户密码信息检测 | 低 | 存在漏洞(发现3处) |
| 44 | 残留手机号信息检测 | 低 | 安全 |
| 通信数据传输安全（6项） | | | |
| 45 | HTTP传输数据风险 | 低 | 存在风险(发现19处) |
| 46 | HTTPS未校验服务器证书漏洞 | 中 | 安全 |
| 47 | HTTPS未校验主机名漏洞 | 中 | 安全 |
| 48 | HTTPS允许任意主机名漏洞 | 中 | 存在漏洞(发现1处) |
| 49 | Webview绕过证书校验漏洞 | 中 | 安全 |
| 50 | HTTP报文信息泄漏风险 | 低 | 未执行 |
| 身份认证安全（3项） | | | |
| 51 | 界面劫持风险 | 中 | 未执行 |
| 52 | 输入监听风险 | 中 | 安全 |
| 53 | 截屏攻击风险 | 中 | 存在风险(发现11处) |
| 内部数据交互安全（12项） | | | |
| 54 | 动态注册Receiver风险 | 中 | 存在风险(发现10处) |
| 55 | Content Provider数据泄露漏洞 | 高 | 未执行 |
| 56 | Activity组件导出风险 | 中 | 存在风险(发现1处) |
| 57 | Service组件导出风险 | 中 | 存在风险(发现2处) |
| 58 | Broadcast Receiver组件导出风险 | 中 | 安全 |
| 59 | Content Provider组件导出风险 | 中 | 安全 |
| 60 | 本地端口开放越权漏洞 | 中 | 未执行 |
| 61 | PendingIntent错误使用Intent风险 | 低 | 安全 |
| 62 | Intent组件隐式调用风险 | 低 | 存在风险(发现10处) |
| 63 | Intent Scheme URL攻击漏洞 | 中 | 安全 |
| 64 | Fragment注入攻击漏洞 | 中 | 安全 |
| 65 | 反射调用风险 | 低 | 存在风险(发现10处) |
| HTML5安全（3项） | | | |
| 66 | Web Storage数据泄露风险 | 低 | 安全 |
| 67 | WebSQL注入漏洞 | 高 | 安全 |
| 68 | InnerHTML的XSS攻击漏洞 | 高 | 安全 |
| 恶意攻击防范能力（13项） | | | |
| 69 | “应用克隆”漏洞攻击风险 | 高 | 存在风险(发现1处) |
| 70 | 动态注入攻击风险 | 高 | 未执行 |
| 71 | Webview远程代码执行漏洞 | 高 | 存在漏洞(发现1处) |
| 72 | 未移除有风险的Webview系统隐藏接口漏洞 | 高 | 存在漏洞(发现1处) |
| 73 | zip文件解压目录遍历漏洞 | 中 | 安全 |
| 74 | 下载任意apk漏洞 | 高 | 安全 |
| 75 | 拒绝服务攻击漏洞 | 中 | 未执行 |
| 76 | 从sdcard加载dex风险 | 中 | 安全 |
| 77 | 从sdcard加载so风险 | 中 | 安全 |
| 78 | 未使用编译器堆栈保护技术风险 | 低 | 存在风险(发现4处) |
| 79 | 未使用地址空间随机化技术风险 | 低 | 安全 |
| 80 | Root设备运行风险 | 低 | 未执行 |
| 81 | 不安全的浏览器调用漏洞 | 中 | 存在漏洞(发现1处) |

# 2. App安全测评结果详情

## 自身安全

### 权限信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 权限分类 | 权限项 | 权限描述 | 权限风险级别 | 权限申请后是否使用 |
| 敏感权限 | WRITE\_EXTERNAL\_STORAGE | 修改/删除SD卡中的内容 | 危险 | 是 |
| 敏感权限 | READ\_EXTERNAL\_STORAGE | 读取SD卡上的内容 | 危险 | 是 |
| 敏感权限 | CAMERA | 访问相机 | 危险 | 是 |
| 敏感权限 | READ\_PHONE\_STATE | 读取手机状态和身份 | 危险 | 是 |
| 敏感权限 | ACCESS\_FINE\_LOCATION | 访问精确位置 | 危险 | 否 |
| 敏感权限 | ACCESS\_COARSE\_LOCATION | 访问大概位置 | 危险 | 否 |
| 敏感权限 | RECORD\_AUDIO | 录音 | 危险 | 否 |
| 普通权限 | CHANGE\_NETWORK\_STATE | 更改网络连接性 | 正常 | 是 |
| 普通权限 | VIBRATE | 控制振动器 | 正常 | 是 |
| 普通权限 | BLUETOOTH\_ADMIN | 蓝牙管理 | 正常 | 是 |
| 普通权限 | BLUETOOTH | 创建蓝牙连接 | 正常 | 是 |
| 普通权限 | ACCESS\_NETWORK\_STATE | 查看网络状态 | 正常 | 是 |
| 普通权限 | ACCESS\_WIFI\_STATE | 查看 WLAN 状态 | 正常 | 是 |
| 普通权限 | INTERNET | 访问网络 | 正常 | 是 |
| 普通权限 | MODIFY\_AUDIO\_SETTINGS | 更改您的音频设置 | 正常 | 否 |
| 普通权限 | RESTART\_PACKAGES | 重启程序 | N/A | 否 |
| 普通权限 | KILL\_BACKGROUND\_PROCESSES | 结束后台进程 | 正常 | 否 |
| 普通权限 | GET\_TASKS | 检索当前运行的应用程序 | 危险 | 否 |
| 普通权限 | SYSTEM\_ALERT\_WINDOW | 显示系统级警报 | 特殊 | 否 |
| 普通权限 | FLASHLIGHT | 控制闪光灯 | N/A | 否 |
| 普通权限 | MOUNT\_UNMOUNT\_FILESYSTEMS | 装载和卸载文件系统 | N/A | 否 |
| 普通权限 | CLEAR\_APP\_CACHE | 删除所有应用程序缓存数据 | 特殊 | 否 |
| 普通权限 | CHANGE\_WIFI\_STATE | 更改 WLAN 状态 | 正常 | 否 |
| 普通权限 | NFC | 允许NFC通讯 | 正常 | 否 |
| 自定义权限 | com.android.launcher.permission.INSTALL\_SHORTCUT | 自定义权限 | N/A | 否 |

### 行为信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 行为项 | 行为描述 | 行为风险等级 | 详细信息 | |
| File\_Write | 写文件 | 低 | 1、文件：org/dom4j/io/STAXEventWriter  2、文件：com/YinanSoft/CardReaders/SerialReader  3、文件：com/YinanSoft/CardReaders/SerialReaderIC  4、文件：com/wintone/Adaptor/CipherAdaptorC2 |
| File\_Del | 删除文件 | 高 | 1、文件：com/jcraft/jsch/ChannelSftp  2、文件：com/ai/smartcrm/update/UpdateManager$3  3、文件：com/ai/smartcrm/activity/MainActivity  4、文件：com/ai/smartcrm/util/DataCleanManager  5、文件：com/wintone/cert/CertBuilder  6、文件：com/wintone/lisence/VersionAuthFileOperate  7、文件：com/wintone/lisence/DateAuthFileOperate  8、文件：com/wintone/lisence/WintoneLSCOperateTools  9、文件：cn/cloudwalk/Utils  10、文件：cn/cloudwalk/libproject/util/FileUtil  11、文件：wintone/idcard/android/IDCardCfg  12、文件：wintone/idcard/android/AuthService |
| Phone\_GetIMEI | 获取IMEI | 低 | 1、文件：com/ctsi/idcertification/CloudReaderClient  2、文件：com/ai/smartcrm/activity/CommonApplication  3、文件：com/ai/smartcrm/nfc/NFCActivity  4、文件：com/sunrise/reader/u  5、文件：com/sunrise/BtReaderClient  6、文件：wintone/idcard/android/RecogService  7、文件：wintone/idcard/android/AuthService  8、文件：wintone/idcard/android/IDCardBean |
| File\_Read | 读文件 | 低 | 1、文件：net/sf/json/groovy/JsonSlurper  2、文件：org/kobjects/xmlrpc/Driver  3、文件：org/dom4j/io/XPP3Reader  4、文件：org/dom4j/io/XPPReader  5、文件：com/jcraft/jsch/OpenSSHConfig  6、文件：com/wintone/lisence/VersionAuthFileOperate  7、文件：com/wintone/lisence/DateAuthFileOperate  8、文件：com/wintone/lisence/DeviceFP  9、文件：com/wintone/lisence/WintoneLSCOperateTools  10、文件：com/wintone/lisence/ProcedureAuthOperate  11、文件：wintone/idcard/android/IDCardCfg  12、文件：wintone/idcard/android/RecogService  13、文件：wintone/idcard/android/AuthService  14、文件：wintone/idcard/android/IDCardBean |
| Data\_Encrypt | 加密数据 | 高 | 1、文件：org/jarjar/apache/commons/codec/digest/DigestUtils  2、文件：com/ctsi/idcertification/custom/SunriseApi$MD5  3、文件：com/jcraft/jsch/jcraft/HMACMD5  4、文件：com/jcraft/jsch/jcraft/HMACSHA1  5、文件：com/jcraft/jsch/jce/SHA1  6、文件：com/jcraft/jsch/jce/MD5  7、文件：com/jcraft/jsch/jce/SHA256  8、文件：com/ai/smartcrm/activity/Md5Util  9、文件：com/wintone/cipher/MD5  10、文件：cn/cloudwalk/libproject/util/Util  11、文件：cn/cloudwalk/libproject/util/ImgUtil  12、文件：com/jcraft/jsch/jcraft/HMAC  13、文件：com/invs/InvsDes3  14、文件：com/Routon/iDRCtLib/Des3  15、文件：com/jcraft/jsch/jce/TripleDESCTR  16、文件：com/jcraft/jsch/jce/BlowfishCBC  17、文件：com/jcraft/jsch/jce/AES256CBC  18、文件：com/jcraft/jsch/jce/ARCFOUR  19、文件：com/jcraft/jsch/jce/ARCFOUR256  20、文件：com/jcraft/jsch/jce/AES128CBC  21、文件：com/jcraft/jsch/jce/TripleDESCBC  22、文件：com/jcraft/jsch/jce/AES128CTR  23、文件：com/jcraft/jsch/jce/AES256CTR  24、文件：com/jcraft/jsch/jce/ARCFOUR128  25、文件：com/jcraft/jsch/jce/AES192CBC  26、文件：com/jcraft/jsch/jce/AES192CTR  27、文件：com/ai/smartcrm/nfc/Des33  28、文件：com/wintone/cipher/RC4  29、文件：com/wintone/cipher/AESWithJCE  30、文件：com/wintone/cipher/AES  31、文件：com/wintone/cipher/RSA  32、文件：com/wintone/cipher/AESofSUN  33、文件：com/yast/yadrly001/secret  34、文件：com/sdses/Des3  35、文件：com/sdses/Util  36、文件：com/jcraft/jsch/jce/HMAC |
| Reflection\_Call | 反射调用 | 高 | 1、文件：org/dom4j/io/SAXContentHandler  2、文件：org/dom4j/bean/BeanMetaData  3、文件：org/json/JSONObject  4、文件：com/invs/Blt2  5、文件：com/invs/ClsUtils  6、文件：com/ai/smartcrm/activity/ListActivity  7、文件：com/ai/smartcrm/camera/FlashlightManager  8、文件：com/YinanSoft/BTDevice/BluetoothCom  9、文件：com/sunrise/h/k  10、文件：com/sunrise/h/c  11、文件：com/sunrise/f/am  12、文件：com/sunrise/reader/b  13、文件：com/sunrise/e/l  14、文件：com/sunrise/e/n |
| Network\_Access | 获取网络连接 | 低 | 1、文件：net/sf/json/groovy/JsonSlurper  2、文件：org/ksoap2/transport/ServiceConnectionSE  3、文件：org/dom4j/io/XPP3Reader  4、文件：org/dom4j/io/XPPReader  5、文件：com/ai/smartcrm/update/UpdateManager$3  6、文件：com/ai/smartcrm/update/UpdateManager$2  7、文件：com/ai/smartcrm/util/URLAvailability  8、文件：com/YinanSoft/Utils/HttpDownloader  9、文件：com/sunrise/f/am  10、文件：com/sunrise/h/j  11、文件：com/zkc/helper/printer/TcpClientClass  12、文件：com/sunrise/reader/ReaderManagerService  13、文件：com/sunrise/reader/f  14、文件：com/sunrise/reader/u$1  15、文件：com/sunrise/reader/n  16、文件：com/sunrise/reader/c  17、文件：com/jcraft/jsch/PortWatcher  18、文件：com/ctsi/idcertification/custom/SunriseApi  19、文件：cn/cloudwalk/libproject/net/ApacheHttpUtil  20、文件：org/opencv/android/AsyncServiceHelper  21、文件：com/ai/smartcrm/common/Constant  22、文件：com/ai/smartcrm/decoding/CaptureActivityHandler  23、文件：cn/cloudwalk/libproject/util/ImgUtil |

### 病毒扫描

|  |  |  |  |
| --- | --- | --- | --- |
| **扫描引擎** | **发现病毒** | **扫描结果** | **病毒详情** |
| CLAMAV | 未发现 | 安全 |  |
| F\_SECURE | 未发现 |
| SOPHOS | 未发现 |

### 敏感词信息

|  |
| --- |
| 未发现敏感词信息 |

### 第三方SDK检测

|  |  |  |
| --- | --- | --- |
| **序号** | **SDK名称** | **SDK描述** |
| 1 | 阿里SDK | com.alibaba |
| 2 | 谷歌SDK | com.google |
| 3 | AndroidSupportLibrary | android.support.v4 |
| 4 | OkHttp | okhttp3.internal |
| 5 | Apache | org.apache |
| 6 | kXML2 | org.kxml2 |
| 7 | Okhttp3 | okhttp3 |
| 8 | Okio | okio |

### 资源文件中的Apk文件

|  |
| --- |
| 该应用的资源文件中不包含Apk文件 |

## 程序源文件安全

### 加固壳识别

|  |  |
| --- | --- |
| **测评目的** | 检测App程序采用了何家厂商的加固方案。 |
| **危险等级** | 高 |
| **危害** | 针对Android平台应用所面临的反编译和二次打包问题，对应用进行加固是目前最有效的解决方案。由于通用加固方案的加固强度较低、加固方式较为普遍，无法有效防止反编译工具的破解，或者容易被脱壳并且反编译，因此，建议采用企业级定制化加固方案，有效地保护源代码安全和防止篡改及二次打包风险。 |
| **测评结果** | 存在风险(发现1处) |
| **测评结果描述** | 该App未使用加固措施。 |
| **测评详细信息** |  |
| **解决方案** | 第三方支持：使用主流的加固厂商提供的专业加固方案。 |

### Java代码反编译风险

|  |  |
| --- | --- |
| **测评目的** | 检测java层代码是否存在源代码被反编译而泄露的风险。 |
| **危险等级** | 高 |
| **危害** | Apk如果未采取有效的保护措施，可能面临被反编译的风险。反编译是将二进制程序转换成人们易读的一种描述语言的形式。反编译的结果是应用程序的代码，这样就暴露了客户端的所有逻辑，比如与服务端的通讯方式，加解密算法、密钥，转账业务流程、软键盘技术实现等等。攻击者可以利用这些信息窃取客户端的敏感数据，包括手机号、密码；截获与服务器之间的通信数据；绕过业务安全认证流程，直接篡改用户账号信息；对服务器接口发起攻击等。 |
| **测评结果** | 存在风险(发现13处) |
| **测评结果描述** | 该Apk可以被反编译后获取源代码。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/activity/MainActivity  2.  [文件]：  com/ai/smartcrm/nfc/NFCActivity  3.  [文件]：  com/ai/smartcrm/scan/CaptureScannerActivity  4.  [文件]：  com/ai/smartcrm/activity/WintoneCameraActivity  5.  [文件]：  wintone/idcard/android/IDCardBean  6.  [文件]：  com/ai/smartcrm/printer/PrintSettingActivity  7.  [文件]：  com/ai/smartcrm/printer/PrintTextActivity  8.  [文件]：  com/ai/smartcrm/activity/ListActivity  9.  [文件]：  cn/cloudwalk/libproject/LiveResultActivity  10.  [文件]：  cn/cloudwalk/libproject/LiveActivity  11.  [文件]：  cn/cloudwalk/libproject/LiveStartActivity  12.  [文件]：  wintone/idcard/android/AuthService  13.  [文件]：  wintone/idcard/android/RecogService |
| **解决方案** | 第三方支持：使用具有防反编译功能的第三方专业加固方案，防止应用被反编译。 |

### So文件破解风险

|  |  |
| --- | --- |
| **测评目的** | 检测Apk中的so文件是否可被破解读取。 |
| **危险等级** | 低 |
| **危害** | So文件为Apk中包含的动态链接库文件，Android利用NDK技术将C/C++语言实现的核心代码编译为so库供Java层调用。So被破解可能导致核心功能的汇编代码甚至源代码泄露，不仅损害开发者的知识产权，并且可能暴露了客户端的核心功能逻辑，攻击者可以利用这些信息窃取客户端的敏感数据，包括手机号、密码；截获与服务器之间的通信数据；绕过业务安全认证流程，直接篡改用户账号信息；对服务器接口发起攻击等。 |
| **测评结果** | 存在风险(发现40处) |
| **测评结果描述** | 该App应用中存在的so文件可被破解，导致核心源码泄露。 |
| **测评详细信息** | 1.  [文件]：  lib/x86/libidReader.so  2.  [文件]：  lib/x86/libinvswlt.so  3.  [文件]：  lib/x86/libcmccreader.so  4.  [文件]：  lib/arm64-v8a/libcloudwalksdk.so  5.  [文件]：  lib/arm64-v8a/libwlt2bmp.so  6.  [文件]：  lib/arm64-v8a/libidReader.so  7.  [文件]：  lib/arm64-v8a/libIDCardReader.so  8.  [文件]：  lib/arm64-v8a/libinvswlt.so  9.  [文件]：  lib/arm64-v8a/libcmccreader.so  10.  [文件]：  lib/mips64/libidReader.so  11.  [文件]：  lib/mips64/libinvswlt.so  12.  [文件]：  lib/mips64/libcmccreader.so  13.  [文件]：  lib/x86\_64/libidReader.so  14.  [文件]：  lib/x86\_64/libcmccreader.so  15.  [文件]：  lib/mips/libidReader.so  16.  [文件]：  lib/mips/libinvswlt.so  17.  [文件]：  lib/mips/libcmccreader.so  18.  [文件]：  lib/armeabi/libcloudwalksdk.so  19.  [文件]：  lib/armeabi/libdewlt-jni.so  20.  [文件]：  lib/armeabi/libwltdecode.so  21.  [文件]：  lib/armeabi/libwlt2bmp.so  22.  [文件]：  lib/armeabi/libserial\_port.so  23.  [文件]：  lib/armeabi/libidReader.so  24.  [文件]：  lib/armeabi/libIDCardReader.so  25.  [文件]：  lib/armeabi/libotgnetcomm.so  26.  [文件]：  lib/armeabi/libinvswlt.so  27.  [文件]：  lib/armeabi/libnfcnetcomm.so  28.  [文件]：  lib/armeabi/libDecodeWlt.so  29.  [文件]：  lib/armeabi/libbluenetcomm.so  30.  [文件]：  lib/armeabi/libAndroidIDCard.so  31.  [文件]：  lib/armeabi/libcmccreader.so  32.  [文件]：  lib/armeabi/libist\_jni.so  33.  [文件]：  lib/armeabi/libWltRS.so  34.  [文件]：  lib/armeabi/libopencv\_java.so  35.  [文件]：  lib/armeabi-v7a/libcloudwalksdk.so  36.  [文件]：  lib/armeabi-v7a/libwlt2bmp.so  37.  [文件]：  lib/armeabi-v7a/libidReader.so  38.  [文件]：  lib/armeabi-v7a/libIDCardReader.so  39.  [文件]：  lib/armeabi-v7a/libinvswlt.so  40.  [文件]：  lib/armeabi-v7a/libcmccreader.so |
| **解决方案** | 第三方支持：使用具有so文件保护功能的第三方专业加固方案，防止so文件被破解。 |

### 篡改和二次打包风险

|  |  |
| --- | --- |
| **测评目的** | 检测客户端的源代码、资源文件、配置文件等被篡改后，是否可以重新打包并正常运行。 |
| **危险等级** | 高 |
| **危害** | Apk篡改后二次打包不仅已经严重危害开发者版权和经济利益，而且也使app用户遭受到不法应用的恶意侵害。对客户端程序添加或修改代码，修改客户端资源图片，配置信息、图标，添加广告，推广自己的产品，再生成新的客户端程序，可导致大量盗版应用的出现分食开发者的收入；恶意的二次打包还能实现应用钓鱼、添加病毒代码、添加恶意代码，从而窃取登录账号密码、支付密码，拦截验证码短信，修改转账目标账号、金额等等。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Janus签名机制漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App程序是否存在Janus签名机制漏洞。 |
| **危险等级** | 高 |
| **危害** | Google披露了一个名为“Janus”的安卓漏洞（漏洞编号：CVE-2017-13156），该漏洞可以让攻击者绕过安卓系统的Signature scheme V1签名机制，用篡改过的APK覆盖原有的应用，并可访问原应用所有的数据，直接对App进行篡改。由于安卓系统的其他安全机制也是建立在签名和校验基础上的，所以可以说该漏洞相当于绕过了安卓系统的整个安全机制。该漏洞的影响范围：安卓5.0-8.0的各个版本系统；使用安卓Signature scheme V1签名的App APK文件。该漏洞的危害：对存储在原手机上的数据进行读取； 对用户的输入做各种监听、拦截、欺诈，引导用户输入密码，转账；更新Android的系统APP，从获得更高的系统权限，甚至root/越狱，为其他攻击做准备。 |
| **测评结果** | 存在漏洞(发现1处) |
| **测评结果描述** | 该App存在Janus签名机制漏洞。 |
| **测评详细信息** |  |
| **解决方案** | 开发者自查：  1.及时校验App APK文件的开始字节，以确保App未被篡改；  2.对应用同时使用Signature scheme V1和Signature scheme V2签名机制 |

### 资源文件泄露风险

|  |  |
| --- | --- |
| **测评目的** | 检测Apk中的资源文件是否可被读取及篡改。 |
| **危险等级** | 低 |
| **危害** | Apk中包含多种类型的资源文件，包括图标，图片，javascript文件等，其中js文件中可能包含资源文件中的重要显示界面及执行，如果js文件被读取可能造成功能逻辑泄露，如果被篡改，可能被植入钓鱼页面或者恶意代码，造成用户的敏感信息泄露。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用中不存在可被读取的js类资源文件。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 应用签名未校验风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序启动时是否校验签名证书。 |
| **危险等级** | 高 |
| **危害** | 签名证书是对App开发者身份的唯一标识，开发者可利用签名证书有效降低App的盗版率。未进行签名证书的App，可能被反编译后进行二次打包。重新打包签名的应用，可能导致App被仿冒盗版，影响其合法收入，甚至可能被添加钓鱼代码、病毒代码、恶意代码，导致用户敏感信息泄露或者恶意攻击。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 代码未混淆风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序的源代码是否已经经过混淆处理。 |
| **危险等级** | 中 |
| **危害** | 代码混淆是一种用来隐藏代码结构及流程的技术，可以增加代码阅读的难度。代码混淆通过将Java代码中的方法名，变量名，类名，包名等这些元素名称改成毫无关联且无意义的名字（如单个字母或者无意义的组合），或者对简单的逻辑分支进行混淆，使攻击者难以找到函数调用的内容，无法掌控app内部实现逻辑，从而增加逆向工程和破解的难度。应用代码如果不经过混淆处理，一旦被反编译，源代码将直接暴露给攻击者，造成程序业务逻辑泄露、加解密算法失效、通信加密失效，攻击者可以利用这些信息窃取客户端的敏感数据，包括账号、密码；绕过业务安全认证流程，直接篡改用户账号信息；对服务器接口发起攻击等。虽然代码混淆并不能真正阻止逆向工程 ，但可以增大反编译代码被解读的难度。 |
| **测评结果** | 存在风险(发现1处) |
| **测评结果描述** | 该App的源代码未做混淆处理。 |
| **测评详细信息** |  |
| **解决方案** | 开发者自查：开发者应在发布程序前，使用Proguard对App程序源代码进行混淆处理，以下是在Eclipse中使用Proguard进行代码混淆的步骤说明：  1.在该App程序的项目下打开"project.properties"文件,在其中添加以下代码以移动代码混淆功能：  proguard.config=${sdk.dir}/tools/proguard/proguard-android.txt:proguard-project.txt  2.在项目根目录下面编辑proguard-project.txt以制定代码混淆规则：  1)使用以下命令对定制混淆部分进行设置:  -libraryjars \*\*.jar （指定要处理的应用程序jar,war,ear和目录所需要的程序库文件）  -dontwarn com.xx.bbb.\*\* （不提示警告）  -keep class com.xx.bbb.\*\* { \*;} （不进行混淆）  -keepclassmembers class \*\* { methods} （对指定类的成员不进行混淆）  -keepclasswithmembers class \*\* { methods} （对指定的类和类的成员不进行混淆）  2)在proguard-project.txt中添加默认设置:  -optimizationpasses 5  -dontskipnonpubliclibraryclassmembers  -printmapping proguardMapping.txt  -optimizations !code/simplification/cast,!field/\*,!class/merging/\*  -keepattributes \*Annotation\*,InnerClasses  -keepattributes Signature  -keepattributes SourceFile,LineNumberTable  -keep public class \* extends android.app.Activity  -keep public class \* extends android.app.Application  -keep public class \* extends android.app.Service  -keep public class \* extends android.content.BroadcastReceiver  -keep public class \* extends android.content.ContentProvider  -keep public class \* extends android.app.backup.BackupAgentHelper  -keep public class \* extends android.preference.Preference  -keep public class \* extends android.view.View  -keep public class com.android.vending.licensing.ILicensingService  -keep class android.support.\*\* {\*;}  -keep public class \* extends android.view.View{  \*\*\* get\*();  void set\*(\*\*\*);  public <init>(android.content.Context);  public <init>(android.content.Context, android.util.AttributeSet);  public <init>(android.content.Context, android.util.AttributeSet, int);  }  -keepclasseswithmembers class \* {  public <init>(android.content.Context, android.util.AttributeSet);  public <init>(android.content.Context, android.util.AttributeSet, int);  }  -keepclassmembers class \* implements java.io  .Serializable {  static final long serialVersionUID;  private static final java.io  .ObjectStreamField[] serialPersistentFields;  private void writeObject(java.io  .ObjectOutputStream);  private void readObject(java.io  .ObjectInputStream);  java.lang.Object writeReplace();  java.lang.Object readResolve();  }  -keep class \*\*.R$\* {  \*;  }  -keepclassmembers class \* {  void \*(\*\*On\*Event);  }  -keepclassmembers class fqcn.of.javascript.interface.for.Webview {  public \*;  }  -keepclassmembers class \* extends android.webkit.WebViewClient {  public void \*(android.webkit.WebView, java.lang.String, android.graphics.Bitmap);  public boolean \*(android.webkit.WebView, java.lang.String);  }  -keepclassmembers class \* extends android.webkit.WebViewClient {  public void \*(android.webkit.WebView, jav.lang.String);  }  3.使用Export方式导出该项目的Apk文件 |

### 使用调试证书发布应用风险

|  |  |
| --- | --- |
| **测评目的** | 检测App是否使用了调试证书发布应用。 |
| **危险等级** | 低 |
| **危害** | 签名证书是验证应用开发者身份的关键标识，可用于判断App是否是由合法开发者发布的正版应用，并且App常使用签名校验作为防止App被二次打包的措施。使用调试证书发布应用，可能导致App无法在应用市场上架，并且debug证书的有效期仅有一年使用；使用debug证书发布的应用可能会出现各个版本的签名证书不一致的情况，这样会导致App应用无法成功升级；同时，证书的不一致性可能造成App使用的签名校验措施频繁改动或者被迫取消，最终导致应用被二次打包。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该应用使用了开发者的release证书发布应用。 |
| **测评详细信息** | Signer #1: Signature: Owner: CN=云南电信智能CRM, OU=中国电信股份有限公司云南分公司, O=中国电信股份有限公司云南分公司, L=昆明市, ST=云南省, C=86 Issuer: CN=云南电信智能CRM, OU=中国电信股份有限公司云南分公司, O=中国电信股份有限公司云南分公司, L=昆明市, ST=云南省, C=86 Serial number: 4640bd06 Valid from: Mon Jul 01 09:42:18 CST 2019 until: Tue Jan 20 09:42:18 CST 2685 Certificate fingerprints: SHA1: 6E:60:ED:68:60:4E:A8:7C:CC:83:9C:2A:03:9D:96:44:21:01:0B:2C SHA256: E8:35:90:43:CE:9A:5C:36:91:E0:00:96:34:AC:AE:8C:25:C2:01:63:14:28:D6:DE:36:0B:7B:A3:28:57:22:A6 Signature algorithm name: SHA256withRSA Subject Public Key Algorithm: 2048-bit RSA key Version: 3 Extensions: #1: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [ KeyIdentifier [ 0000: 62 B0 24 13 33 45 B2 67 0E 16 A6 53 1B 8E 0B 4A b.$.3E.g...S...J 0010: 1F 02 E1 C6 .... ] ] |
| **解决方案** |  |

### 仅使用Java代码风险

|  |  |
| --- | --- |
| **测评目的** | 检测App是否仅使用了Java代码 |
| **危险等级** | 低 |
| **危害** | 在Android开发本地代码时，有两种方式，一种是使用javah生成头文件，然后编辑源代码，另一种不用生成头文件，直接编辑代码后，使用RegisterNatives方法进行注册，是运行在JVM外的Native代码。针对第一种方式，使用javah生成头文件，枚举java声明的native方法，事实上可以查到对应的函数，使用工具轻易获取源码，造成代码泄露。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App不是完全使用Java代码 |
| **测评详细信息** |  |
| **解决方案** |  |

### 启动隐藏服务风险

|  |  |
| --- | --- |
| **测评目的** | 检测App是否启动了隐藏的服务。 |
| **危险等级** | 低 |
| **危害** | 一般的应用会以界面形式启动程序，隐藏程序启动Activity的应用易被安全检测工具误识别为恶意应用木马、病毒等，也可能存在感染恶意木马和病毒的风险。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App没有启动隐藏的服务。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 应用签名算法不安全风险

|  |  |
| --- | --- |
| **测评目的** | 检测App是否使用了不安全的应用签名算法。 |
| **危险等级** | 低 |
| **危害** | 在签署数字证书时，哈希算法的完整性是决定证书安全性的关键因素。哈希算法的弱点可能导致攻击者在某些情况下能够获得伪造的证书。其中，普遍使用的SHA-1已经过时因而不再推荐使用，基于MD5的签名的支持也已在2012年初停止，建议使用更安全的签名算法，如SHA-2（其中包括SHA-256和SHA-512）。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该应用使用了安全的应用签名算法。 |
| **测评详细信息** |  |
| **解决方案** |  |

## 本地数据存储安全

### Webview明文存储密码风险

|  |  |
| --- | --- |
| **测评目的** | 检测App应用的Webview组件中是否使用明文保存用户名及密码。 |
| **危险等级** | 高 |
| **危害** | Android的Webview组件中默认打开了提示用户是否保存密码的功能，如果用户选择保存，用户名和密码将被明文存储到该应用目录databases/webview.db中。而本地明文存储的用户名和密码，不仅会被该应用随意浏览，其他恶意程序也可能通过提权或者root的方式访问该应用的webview数据库，从而窃取用户登录过的用户名信息以及密码。 |
| **测评结果** | 存在风险(发现1处) |
| **测评结果描述** | 该App应用的Webview组件中未设置关闭自动保存密码功能，用户名和密码可能被明文存储。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private initWebView()V |
| **解决方案** | 开发者自查：通过设置WebView.getSettings().setSavePassword(false)关闭webview组件的保存密码功能。 |

### Webview File同源策略绕过漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测Apk中WebView的file域协议是否存在同源策略绕过的漏洞。 |
| **危险等级** | 高 |
| **危害** | JavaScript的延时执行能够绕过file协议的同源检查，并能够访问受害应用的所有私有文件，即通过WebView对Javascript的延时执行和将当前Html文件删除掉并软连接指向其他文件就可以读取到被符号链接所指的文件，然后通过JavaScript再次读取HTML文件，即可获取到被符号链接所指的文件。大多数使用WebView的应用都会受到该漏洞的影响，恶意应用通过该漏洞，可在无特殊权限下盗取应用的任意私有文件，尤其是浏览器，可通过利用该漏洞，获取到浏览器所保存的密码、Cookie、收藏夹以及历史记录等敏感信息，从而造成敏感信息泄露。 |
| **测评结果** | 存在漏洞(发现1处) |
| **测评结果描述** | 该Apk程序存在webview File同源策略绕过的漏洞。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private initWebView()V |
| **解决方案** | 开发者自查：  1. 将不必要导出的组件设置为不导出，并显式设置所注册组件的“android:exported”属性为false；  2. 如果需要导出组件，禁止使用File域  WebView.getSettings.setAllowFileAccess(false);  3. 如果需要使用File协议，禁止File协议调用JavaScript：  WebView.getSettings.setJavaScriptEnabled(false) |

### 明文数字证书风险

|  |  |
| --- | --- |
| **测评目的** | 检测客户端是否包含明文存储的数字证书文件。 |
| **危险等级** | 中 |
| **危害** | Apk中使用的数字证书可被用来校验服务器的合法身份，以及在与服务器进行通信的过程中对传输数据进行加密、解密运算，保证传输数据的保密性、完整性。明文存储的数字证书如果被篡改，客户端可能连接到假冒的服务端上，导致用户名、密码等信息被窃取；如果明文证书被盗取，可能造成传输数据被截获解密，用户信息泄露，或者伪造客户端向服务器发送请求，篡改服务器中的用户数据或造成服务器响应异常。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该Apk 中不存在明文存储的数字证书文件。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 调试日志函数调用风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序中是否调用了调试日志函数。 |
| **危险等级** | 低 |
| **危害** | 调试日志函数可能输出重要的日志文件，其中包含的信息可能导致客户端用户信息泄露，暴露客户端代码逻辑等，为发起攻击提供便利，例如：Activity的组件名，是Activity劫持需要的信息；通信交互的日志，会成为发动服务器攻击的依据；跟踪的变量值，可能泄露一些敏感数据，输入的账号、密码等。 |
| **测评结果** | 存在风险(发现435处) |
| **测评结果描述** | 该App存在调试日志函数的调用，可能发生重要日志信息泄露的风险。 |
| **测评详细信息** | 为避免显示内容过长，该项检测在此报告中只显示50处发现问题点，更多详情请在系统中查看。  1.  [文件]：  org/xmlpull/v1/XmlPullParserException  [方法]：  public printStackTrace()V  2.  [文件]：  org/opencv/android/JavaCameraView  [方法]：  protected connectCamera(II)Z  3.  [文件]：  org/opencv/android/JavaCameraView  [方法]：  protected disconnectCamera()V  4.  [文件]：  org/opencv/android/JavaCameraView  [方法]：  protected initializeCamera(II)Z  5.  [文件]：  org/opencv/android/JavaCameraView  [方法]：  public onPreviewFrame([BLandroid/hardware/Camera;)V  6.  [文件]：  org/opencv/android/BaseLoaderCallback  [方法]：  public onManagerConnected(I)V  7.  [文件]：  org/opencv/android/AsyncServiceHelper$1$2  [方法]：  public cancel()V  8.  [文件]：  org/opencv/android/AsyncServiceHelper$1$2  [方法]：  public install()V  9.  [文件]：  org/opencv/android/AsyncServiceHelper$1$2  [方法]：  public wait\_install()V  10.  [文件]：  org/opencv/android/AsyncServiceHelper$1$1  [方法]：  public cancel()V  11.  [文件]：  org/opencv/android/AsyncServiceHelper$1$1  [方法]：  public install()V  12.  [文件]：  org/opencv/android/AsyncServiceHelper$1$1  [方法]：  public wait\_install()V  13.  [文件]：  org/opencv/android/AsyncServiceHelper  [方法]：  protected static InstallService(Landroid/content/Context;Lorg/opencv/android/LoaderCallbackInterface;)V  14.  [文件]：  org/opencv/android/AsyncServiceHelper  [方法]：  private initOpenCVLibs(Ljava/lang/String;Ljava/lang/String;)Z  15.  [文件]：  org/opencv/android/AsyncServiceHelper  [方法]：  private loadLibrary(Ljava/lang/String;)Z  16.  [文件]：  org/opencv/android/NativeCameraView$CameraWorker  [方法]：  public run()V  17.  [文件]：  org/opencv/android/NativeCameraView  [方法]：  private initializeCamera(II)Z  18.  [文件]：  org/opencv/android/AsyncServiceHelper$3  [方法]：  public cancel()V  19.  [文件]：  org/opencv/android/AsyncServiceHelper$3  [方法]：  public install()V  20.  [文件]：  org/opencv/android/AsyncServiceHelper$2  [方法]：  public cancel()V  21.  [文件]：  org/opencv/android/AsyncServiceHelper$2  [方法]：  public install()V  22.  [文件]：  org/opencv/android/AsyncServiceHelper$2  [方法]：  public wait\_install()V  23.  [文件]：  org/opencv/android/StaticHelper  [方法]：  public static initOpenCV()Z  24.  [文件]：  org/opencv/android/StaticHelper  [方法]：  private static initOpenCVLibs(Ljava/lang/String;)Z  25.  [文件]：  org/opencv/android/StaticHelper  [方法]：  private static loadLibrary(Ljava/lang/String;)Z  26.  [文件]：  org/opencv/android/JavaCameraView$CameraWorker  [方法]：  public run()V  27.  [文件]：  org/opencv/android/AsyncServiceHelper$1  [方法]：  public onServiceConnected(Landroid/content/ComponentName;Landroid/os/IBinder;)V  28.  [文件]：  org/opencv/android/CameraBridgeViewBase$CvCameraViewListenerAdapter  [方法]：  public onCameraFrame(Lorg/opencv/android/CameraBridgeViewBase$CvCameraViewFrame;)Lorg/opencv/core/Mat;  29.  [文件]：  org/opencv/android/FpsMeter  [方法]：  public draw(Landroid/graphics/Canvas;FF)V  30.  [文件]：  org/opencv/android/FpsMeter  [方法]：  public measure()V  31.  [文件]：  org/opencv/android/CameraBridgeViewBase  [方法]：  public constructor <init>(Landroid/content/Context;Landroid/util/AttributeSet;)V  32.  [文件]：  org/opencv/android/CameraBridgeViewBase  [方法]：  protected deliverAndDrawFrame(Lorg/opencv/android/CameraBridgeViewBase$CvCameraViewFrame;)V  33.  [文件]：  org/opencv/android/CameraBridgeViewBase  [方法]：  public surfaceChanged(Landroid/view/SurfaceHolder;III)V  34.  [文件]：  org/kobjects/util/ChainedRuntimeException  [方法]：  public printStackTrace()V  35.  [文件]：  org/dom4j/io/SAXHelper  [方法]：  public static createXMLReader(Z)Lorg/xml/sax/XMLReader;  36.  [文件]：  org/dom4j/datatype/DatatypeDocumentFactory  [方法]：  protected loadSchema(Lorg/dom4j/Document;Ljava/lang/String;)V  37.  [文件]：  org/dom4j/datatype/DatatypeDocumentFactory  [方法]：  protected loadSchema(Lorg/dom4j/Document;Ljava/lang/String;Lorg/dom4j/Namespace;)V  38.  [文件]：  org/dom4j/datatype/SchemaParser  [方法]：  private declared-synchronized internalBuild(Lorg/dom4j/Document;)V  39.  [文件]：  org/dom4j/DocumentException  [方法]：  public printStackTrace()V  40.  [文件]：  pax/util/a  [方法]：  private a()Z  41.  [文件]：  com/ctsi/idcertification/custom/SunriseApi  [方法]：  public auth(Lcom/ctsi/idcertification/entity/AuthInfo;)V  42.  [文件]：  com/ctsi/idcertification/custom/SunriseApi  [方法]：  public getDevicesProperty(I)Lcom/ctsi/idcertification/entity/ReaderProperty;  43.  [文件]：  com/ctsi/idcertification/CloudReaderClient$6  [方法]：  public run()V  44.  [文件]：  com/ctsi/idcertification/CloudReaderClient  [方法]：  private ReadCard(Lcom/ctsi/idcertification/entity/AuthInfo;I)V  45.  [文件]：  com/ctsi/idcertification/CloudReaderClient  [方法]：  public CloudReadCert(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;ILandroid/nfc/Tag;)Ljava/util/Map;  46.  [文件]：  com/ctsi/idcertification/CloudReaderClient$4  [方法]：  public run()V  47.  [文件]：  com/invs/ClsUtils  [方法]：  public static printAllInform(Ljava/lang/Class;)V  48.  [文件]：  com/invs/ClsUtils  [方法]：  public static setPin(Ljava/lang/Class;Landroid/bluetooth/BluetoothDevice;Ljava/lang/String;)Z  49.  [文件]：  com/invs/invswlt  [方法]：  static constructor <clinit>()V  50.  [文件]：  com/Routon/iDRCtLib/BtReaderClient  [方法]：  private recvData([B)I  51.  [文件]：  com/Routon/iDRCtLib/BtReaderClient  [方法]：  private sendData([B)I  52.  [文件]：  com/Routon/iDRCtLib/BtReaderClient  [方法]：  public connectBt(Ljava/lang/String;)Ljava/lang/Boolean;  53.  [文件]：  com/Routon/iDRCtLib/BtReaderClient  [方法]：  public disconnectBt()Ljava/lang/Boolean;  54.  [文件]：  com/pax/api/PiccManager  [方法]：  public m1Authority(BB[B[B)V  55.  [文件]：  com/pax/api/PiccManager  [方法]：  public m1Operate(BB[BB)V  56.  [文件]：  com/pax/api/PiccManager  [方法]：  public m1ReadBlock(B)[B  57.  [文件]：  com/pax/api/PiccManager  [方法]：  public m1WriteBlock(B[B)V  58.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccClose()V  59.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccCmdExchange([BI)[B  60.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccDetect(B)Lcom/pax/api/PiccManager$PiccCardInfo;  61.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccInitFelica(BB)V  62.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccIsoCommand(BLcom/pax/api/model/APDU\_SEND;)Lcom/pax/api/model/APDU\_RESP;  63.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccLight(BB)V  64.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccOpen()V  65.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccRemove(BB)V  66.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccSetup(BLcom/pax/api/model/PICC\_PARA;)Lcom/pax/api/model/PICC\_PARA;  67.  [文件]：  com/pax/api/PiccManager  [方法]：  public piccSetupIdCard(BI)V  68.  [文件]：  com/wch/wchusbdriver/CH34xAndroidDriver$1  [方法]：  public onReceive(Landroid/content/Context;Landroid/content/Intent;)V  69.  [文件]：  com/wch/wchusbdriver/CH34xAndroidDriver  [方法]：  public ResumeUsbList()I  70.  [文件]：  com/zkc/helper/printer/BlueToothService$WriteThread  [方法]：  public run()V  71.  [文件]：  com/zkc/helper/printer/TcpClientClass$TCPServerThread  [方法]：  public run()V  72.  [文件]：  com/zkc/helper/printer/TcpClientClass  [方法]：  public Connect(Ljava/lang/String;I)V  73.  [文件]：  com/zkc/helper/printer/TcpClientClass  [方法]：  public DisConnect()V  74.  [文件]：  com/zkc/helper/printer/TcpClientClass  [方法]：  public SendData([B)V  75.  [文件]：  com/zkc/helper/printer/BlueToothService$AcceptThread  [方法]：  public constructor <init>(Lcom/zkc/helper/printer/BlueToothService;)V  76.  [文件]：  com/zkc/helper/printer/BlueToothService$AcceptThread  [方法]：  public cancel()V  77.  [文件]：  com/zkc/helper/printer/BlueToothService$AcceptThread  [方法]：  public run()V  78.  [文件]：  com/zkc/helper/printer/BlueToothService$ConnectedThread  [方法]：  public constructor <init>(Lcom/zkc/helper/printer/BlueToothService;Landroid/bluetooth/BluetoothSocket;)V  79.  [文件]：  com/zkc/helper/printer/BlueToothService$ConnectedThread  [方法]：  public cancel()V  80.  [文件]：  com/zkc/helper/printer/BlueToothService$ConnectedThread  [方法]：  public run()V  81.  [文件]：  com/zkc/helper/printer/BlueToothService$ConnectedThread  [方法]：  public write([B)V  82.  [文件]：  com/zkc/helper/printer/BlueToothService$ConnectThread  [方法]：  public constructor <init>(Lcom/zkc/helper/printer/BlueToothService;Landroid/bluetooth/BluetoothDevice;)V  83.  [文件]：  com/zkc/helper/printer/BlueToothService$ConnectThread  [方法]：  public cancel()V  84.  [文件]：  com/zkc/helper/printer/BlueToothService$ConnectThread  [方法]：  public run()V  85.  [文件]：  com/zkc/helper/printer/BlueToothService  [方法]：  private Write([B)Z  86.  [文件]：  com/zkc/helper/printer/BlueToothService  [方法]：  public declared-synchronized start()V  87.  [文件]：  com/zkc/helper/printer/BlueToothService  [方法]：  public declared-synchronized stop()V  88.  [文件]：  com/ai/smartcrm/update/DialogHelper  [方法]：  public static SetDialogShowing(Landroid/content/DialogInterface;Z)V  89.  [文件]：  com/ai/smartcrm/update/UpdateManager  [方法]：  private getCurVersion()V  90.  [文件]：  com/ai/smartcrm/update/UpdateManager$2  [方法]：  public run()V  91.  [文件]：  com/ai/smartcrm/ocrengine/ImageUtils  [方法]：  public static saveBitmapToFile(Landroid/graphics/Bitmap;Ljava/lang/String;)V  92.  [文件]：  com/ai/smartcrm/ocrengine/OcrEngine  [方法]：  public static doBackbyPath(Landroid/content/Context;Ljava/lang/String;Lcom/ai/smartcrm/ocrengine/IDCard;)Z  93.  [文件]：  com/ai/smartcrm/ocrengine/OcrEngine  [方法]：  public static doFrontbyPath(Landroid/content/Context;Ljava/lang/String;Lcom/ai/smartcrm/ocrengine/IDCard;)Z  94.  [文件]：  com/ai/smartcrm/activity/MainActivity$MyWebChromeClient  [方法]：  public openFileChooser(Landroid/webkit/ValueCallback;Ljava/lang/String;Ljava/lang/String;)V  95.  [文件]：  com/ai/smartcrm/activity/ListActivity$8  [方法]：  public run()V  96.  [文件]：  com/ai/smartcrm/activity/WintoneCameraActivity  [方法]：  private doOCRbypath(Ljava/lang/String;)V  97.  [文件]：  com/ai/smartcrm/activity/WintoneCameraActivity  [方法]：  protected onActivityResult(IILandroid/content/Intent;)V  98.  [文件]：  com/ai/smartcrm/activity/ListActivity$2$1  [方法]：  public onBtState(Z)V  99.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private clearCookies()V  100.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private exec(ILjava/lang/String;)V  101.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  public static getBitmapFromUri(Landroid/net/Uri;Landroid/content/Context;)Landroid/graphics/Bitmap;  102.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private getUrl()Ljava/lang/String;  103.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private initWebView()V  104.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private temporaryCaptureToSave(Ljava/lang/String;Landroid/net/Uri;)Landroid/net/Uri;  105.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  public clearWebViewCache()V  106.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  public deleteFile(Ljava/io/File;)V  107.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  protected onActivityResult(IILandroid/content/Intent;)V  108.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  public onMenuItemClick(Landroid/view/MenuItem;)Z  109.  [文件]：  com/ai/smartcrm/activity/CommonApplication  [方法]：  public init()V  110.  [文件]：  com/ai/smartcrm/activity/ListActivity$1  [方法]：  public handleMessage(Landroid/os/Message;)V  111.  [文件]：  com/ai/smartcrm/activity/MainActivity$1  [方法]：  public handleMessage(Landroid/os/Message;)V  112.  [文件]：  com/ai/smartcrm/activity/CrashHandler  [方法]：  private saveCrashInfo2File(Ljava/lang/Throwable;)Ljava/lang/String;  113.  [文件]：  com/ai/smartcrm/activity/CrashHandler  [方法]：  public collectDeviceInfo(Landroid/content/Context;)V  114.  [文件]：  com/ai/smartcrm/activity/CrashHandler  [方法]：  public uncaughtException(Ljava/lang/Thread;Ljava/lang/Throwable;)V  115.  [文件]：  com/ai/smartcrm/activity/FileOperationsJava  [方法]：  public byte2File([BLjava/lang/String;Ljava/lang/String;)V  116.  [文件]：  com/ai/smartcrm/activity/FileOperationsJava  [方法]：  public stringtoBitmap(Ljava/lang/String;)Landroid/graphics/Bitmap;  117.  [文件]：  com/ai/smartcrm/activity/ListActivity$7  [方法]：  public onBtState(Z)V  118.  [文件]：  com/ai/smartcrm/activity/ListActivity$2  [方法]：  public onItemClick(Landroid/widget/AdapterView;Landroid/view/View;IJ)V  119.  [文件]：  com/ai/smartcrm/activity/ListActivity  [方法]：  private doDiscovery()V  120.  [文件]：  com/ai/smartcrm/activity/ListActivity  [方法]：  private getSignature()Ljava/lang/String;  121.  [文件]：  com/ai/smartcrm/activity/ListActivity  [方法]：  private parseCardInfo([B)Lcom/invs/InvsIdCard;  122.  [文件]：  com/ai/smartcrm/activity/ListActivity  [方法]：  private updateResultToUI(Ljava/lang/String;)V  123.  [文件]：  com/ai/smartcrm/activity/ListActivity  [方法]：  public readCardSuccess(Ljava/lang/String;)V  124.  [文件]：  com/ai/smartcrm/activity/MainActivity$JavaScriptInterface  [方法]：  public blPrint(Ljava/lang/String;)V  125.  [文件]：  com/ai/smartcrm/camera/CameraManager  [方法]：  public getFramingRect()Landroid/graphics/Rect;  126.  [文件]：  com/ai/smartcrm/camera/CameraConfigurationManager  [方法]：  private static findBestPreviewSizeValue(Ljava/lang/CharSequence;Landroid/graphics/Point;)Landroid/graphics/Point;  127.  [文件]：  com/ai/smartcrm/camera/CameraConfigurationManager  [方法]：  private static getCameraResolution(Landroid/hardware/Camera$Parameters;Landroid/graphics/Point;)Landroid/graphics/Point;  128.  [文件]：  com/ai/smartcrm/camera/CameraConfigurationManager  [方法]：  private setZoom(Landroid/hardware/Camera$Parameters;)V  129.  [文件]：  com/ai/smartcrm/camera/CameraConfigurationManager  [方法]：  initFromCameraParameters(Landroid/hardware/Camera;)V  130.  [文件]：  com/ai/smartcrm/camera/CameraConfigurationManager  [方法]：  setDesiredCameraParameters(Landroid/hardware/Camera;)V  131.  [文件]：  com/ai/smartcrm/camera/PreviewCallback  [方法]：  public onPreviewFrame([BLandroid/hardware/Camera;)V  132.  [文件]：  com/ai/smartcrm/camera/AutoFocusCallback  [方法]：  public onAutoFocus(ZLandroid/hardware/Camera;)V  133.  [文件]：  com/ai/smartcrm/camera/FlashlightManager  [方法]：  static constructor <clinit>()V  134.  [文件]：  com/ai/smartcrm/camera/FlashlightManager  [方法]：  private static varargs invoke(Ljava/lang/reflect/Method;Ljava/lang/Object;[Ljava/lang/Object;)Ljava/lang/Object;  135.  [文件]：  com/ai/smartcrm/camera/FlashlightManager  [方法]：  private static maybeForName(Ljava/lang/String;)Ljava/lang/Class;  136.  [文件]：  com/ai/smartcrm/camera/FlashlightManager  [方法]：  private static varargs maybeGetMethod(Ljava/lang/Class;Ljava/lang/String;[Ljava/lang/Class;)Ljava/lang/reflect/Method;  137.  [文件]：  com/ai/smartcrm/common/SharedPreferencesUtils  [方法]：  private getValue(Ljava/lang/String;Ljava/lang/Class;Landroid/content/SharedPreferences;)Ljava/lang/Object;  138.  [文件]：  com/ai/smartcrm/nfc/NFCActivity$1  [方法]：  public handleMessage(Landroid/os/Message;)V  139.  [文件]：  com/ai/smartcrm/nfc/FileOperationsJava  [方法]：  public byte2File([BLjava/lang/String;Ljava/lang/String;)V  140.  [文件]：  com/ai/smartcrm/nfc/FileOperationsJava  [方法]：  public stringtoBitmap(Ljava/lang/String;)Landroid/graphics/Bitmap;  141.  [文件]：  com/ai/smartcrm/nfc/NFCActivity  [方法]：  private getSignature()Ljava/lang/String;  142.  [文件]：  com/ai/smartcrm/nfc/NFCActivity  [方法]：  protected getBean(Ljava/lang/String;)Lcom/ai/smartcrm/nfc/IdCard\_Bean;  143.  [文件]：  com/ai/smartcrm/nfc/NFCActivity  [方法]：  public getLocalIpAddress()Ljava/lang/String;  144.  [文件]：  com/ai/smartcrm/nfc/NFCActivity  [方法]：  public pageSure(Landroid/view/View;)V  145.  [文件]：  com/ai/smartcrm/decoding/DecodeHandler  [方法]：  private decode([BII)V  146.  [文件]：  com/ai/smartcrm/decoding/CaptureActivityHandler  [方法]：  public handleMessage(Landroid/os/Message;)V  147.  [文件]：  com/ai/smartcrm/util/DataCleanManager  [方法]：  public static clearAppUserData(Ljava/lang/String;)Ljava/lang/Process;  148.  [文件]：  com/ai/smartcrm/util/DataCleanManager  [方法]：  public static execRuntimeProcess(Ljava/lang/String;)Ljava/lang/Process;  149.  [文件]：  com/ai/smartcrm/util/URLAvailability  [方法]：  public static declared-synchronized isConnect(Ljava/lang/String;)Z  150.  [文件]：  com/ai/smartcrm/util/SFTPUtil  [方法]：  public static main([Ljava/lang/String;)V  151.  [文件]：  com/ai/smartcrm/util/SFTPUtil  [方法]：  public connect()V  152.  [文件]：  com/ai/smartcrm/util/SFTPUtil  [方法]：  public disconnect()V  153.  [文件]：  com/ai/smartcrm/util/SFTPUtil  [方法]：  public download(Ljava/lang/String;)Ljava/io/InputStream;  154.  [文件]：  com/ai/smartcrm/util/SFTPUtil  [方法]：  public upload(Ljava/io/InputStream;Ljava/lang/String;)V  155.  [文件]：  com/ai/smartcrm/printer/PrintTextActivity$2  [方法]：  public handleMessage(Landroid/os/Message;)V  156.  [文件]：  com/YinanSoft/CardReaders/IDCardReader  [方法]：  public fromJni([B)Z  157.  [文件]：  com/YinanSoft/CardReaders/IDCardReader  [方法]：  protected openSerialPort(Ljava/io/File;II)Z  158.  [文件]：  com/YinanSoft/CardReaders/SerialReader  [方法]：  public InitReader([B)Z  159.  [文件]：  com/YinanSoft/CardReaders/UsbReader  [方法]：  private SendAndRecv2([B)Ljava/lang/String;  160.  [文件]：  com/YinanSoft/CardReaders/UsbReader  [方法]：  public InitReader([BLcom/YinanSoft/BTDevice/IUsbReaderCallback;)Z  161.  [文件]：  com/YinanSoft/CardReaders/UsbReader  [方法]：  public ReadBaseCardInfo([Ljava/lang/String;)Lcom/YinanSoft/CardReaders/IDCardInfo;  162.  [文件]：  com/YinanSoft/CardReaders/UsbReader  [方法]：  public ReadSAMID([Ljava/lang/String;)Ljava/lang/String;  163.  [文件]：  com/YinanSoft/Utils/CertImgDisposeUtils  [方法]：  private getDescribeBitmap(I)Landroid/graphics/Bitmap;  164.  [文件]：  com/YinanSoft/Utils/CertImgDisposeUtils  [方法]：  public creatBitmap(Lcom/YinanSoft/CardReaders/IDCardInfo;)Landroid/graphics/Bitmap;  165.  [文件]：  com/YinanSoft/Utils/HttpDownloader  [方法]：  public static isConnect(Landroid/content/Context;)Z  166.  [文件]：  com/YinanSoft/BTDevice/BluetoothCom  [方法]：  public static bluetoothConnect(Ljava/lang/String;)I  167.  [文件]：  com/wintone/lisence/CDKey  [方法]：  public cdKey(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String;  168.  [文件]：  com/wintone/lisence/EncryptFile  [方法]：  public encryptFiles(Ljava/lang/String;Ljava/io/File;Ljava/lang/String;)I  169.  [文件]：  com/wintone/lisence/EncryptFile  [方法]：  public encryptString(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String;  170.  [文件]：  com/wintone/lisence/DateAuthFileOperate  [方法]：  private readOldDateAuthFile(Ljava/lang/String;)[Ljava/lang/String;  171.  [文件]：  com/wintone/lisence/WintoneLSCOperateTools  [方法]：  public static ModifyNumberInAuthFileByProjectType(Ljava/lang/String;)Ljava/lang/Boolean;  172.  [文件]：  com/yast/yadrly001/MyApplication  [方法]：  public onConnectFail()V  173.  [文件]：  com/yast/yadrly001/MyApplication  [方法]：  public onConnectLost()V  174.  [文件]：  com/yast/yadrly001/MyApplication  [方法]：  public onConnectSuccess()V  175.  [文件]：  com/yast/yadrly001/MyApplication  [方法]：  public setConnect(Z)V  176.  [文件]：  com/yast/yadrly001/BluetoothChatService  [方法]：  private declared-synchronized setState(I)V  177.  [文件]：  com/yast/yadrly001/BluetoothChatService  [方法]：  public declared-synchronized connect(Landroid/bluetooth/BluetoothDevice;)V  178.  [文件]：  com/yast/yadrly001/BluetoothChatService  [方法]：  public connect1(Landroid/bluetooth/BluetoothDevice;)Z  179.  [文件]：  com/yast/yadrly001/BluetoothChatService  [方法]：  public declared-synchronized connected(Landroid/bluetooth/BluetoothSocket;Landroid/bluetooth/BluetoothDevice;)V  180.  [文件]：  com/yast/yadrly001/BluetoothChatService  [方法]：  public connected1(Landroid/bluetooth/BluetoothSocket;Landroid/bluetooth/BluetoothDevice;)V  181.  [文件]：  com/yast/yadrly001/BluetoothChatService  [方法]：  public declared-synchronized stop()V  182.  [文件]：  com/yast/yadrly001/MyApplication$1  [方法]：  public handleMessage(Landroid/os/Message;)V  183.  [文件]：  com/yast/yadrly001/BluetoothChatService$ConnectThread  [方法]：  public constructor <init>(Lcom/yast/yadrly001/BluetoothChatService;Landroid/bluetooth/BluetoothDevice;)V  184.  [文件]：  com/yast/yadrly001/BluetoothChatService$ConnectThread  [方法]：  public cancel()V  185.  [文件]：  com/yast/yadrly001/BluetoothChatService$ConnectThread  [方法]：  public run()V  186.  [文件]：  com/yast/yadrly001/BluetoothChatService$ConnectedThread  [方法]：  public constructor <init>(Lcom/yast/yadrly001/BluetoothChatService;Landroid/bluetooth/BluetoothSocket;)V  187.  [文件]：  com/yast/yadrly001/BluetoothChatService$ConnectedThread  [方法]：  public cancel()V  188.  [文件]：  com/yast/yadrly001/BluetoothChatService$ConnectedThread  [方法]：  public run()V  189.  [文件]：  com/yast/yadrly001/BluetoothChatService$ConnectedThread  [方法]：  public declared-synchronized write([B)V  190.  [文件]：  com/yast/yadrly001/BtReaderClient$ConnectBroadcast  [方法]：  public onReceive(Landroid/content/Context;Landroid/content/Intent;)V  191.  [文件]：  com/yast/yadrly001/BtReaderClient  [方法]：  private writexml()Ljava/lang/String;  192.  [文件]：  com/yast/yadrly001/BtReaderClient  [方法]：  public TransApduData(Ljava/lang/String;[Ljava/lang/String;[II)Z  193.  [文件]：  com/yast/yadrly001/BtReaderClient  [方法]：  public read()Lcom/yast/yadrly001/People;  194.  [文件]：  com/yast/yadrly001/BtReaderClient  [方法]：  public readsamid()Ljava/lang/String;  195.  [文件]：  com/yast/yadrly001/BtReaderClient  [方法]：  public writekey(Ljava/lang/String;)I  196.  [文件]：  com/rwin/custom/PrinterCustom  [方法]：  private doRet(I)I  197.  [文件]：  com/rwin/custom/PrinterCustom  [方法]：  private initByBlack()I  198.  [文件]：  com/rwin/custom/PrinterCustom  [方法]：  private isFindNewBlackLine(I)Z  199.  [文件]：  com/rwin/custom/PrinterCustom  [方法]：  private print(Ljava/lang/String;ILjava/lang/String;)I  200.  [文件]：  com/rwin/custom/PrinterCustom  [方法]：  public printBJ(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/util/LinkedHashMap;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)I  201.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  private powerOffSIM()I  202.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  private readICCIDData(I)Ljava/lang/String;  203.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  private verifyIMSI2(ILjava/lang/String;)I  204.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  private writeIMSI(ILjava/lang/String;)I  205.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  private writeMobileNumber(ILjava/lang/String;)I  206.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  private writeSMSCNumber(ILjava/lang/String;)I  207.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  public openAndClose()V  208.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  public requestAndWait(Ljava/lang/String;[B[BILjava/lang/String;)Z  209.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  public sendAndRecv(Ljava/lang/String;I[B[BI)I  210.  [文件]：  com/rwin/pub/RWSIMCard  [方法]：  public sendAndRecv1111(Ljava/lang/String;I[B[BI)I  211.  [文件]：  com/rwin/pub/I2CSIMCard  [方法]：  private gzGetSimInfo(Ljava/lang/String;)Ljava/lang/String;  212.  [文件]：  com/rwin/pub/I2CSIMCard  [方法]：  private powerOffSIM()I  213.  [文件]：  com/rwin/pub/I2CSIMCard  [方法]：  public readICCID(I)Ljava/lang/String;  214.  [文件]：  com/rwin/pub/I2CSIMCard  [方法]：  public readIMSI(I)Ljava/lang/String;  215.  [文件]：  com/rwin/pub/I2CSIMCard  [方法]：  public writeNumber(ILjava/lang/String;Ljava/lang/String;Ljava/lang/String;)I  216.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  private checkAppKey([B)I  217.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  private checkMasterKey([B)I  218.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  private powerOffSIM()I  219.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  public changePinCode([BB[BB[BB[B)B  220.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  public checkPinCode([BB[BB[B)B  221.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  public getDesData([BBB[BB[B)B  222.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  public psam\_Detect()B  223.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  public readPsamCardId(B[B[B[B)B  224.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  public readXJSIMCardId(I)Ljava/lang/String;  225.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  public requestAndWait(Ljava/lang/String;[B[BILjava/lang/String;)Z  226.  [文件]：  com/rwin/pub/psamRWCard  [方法]：  public sendAndRecv(Ljava/lang/String;I[B[BI)I  227.  [文件]：  com/rwin/pub/BoxManager  [方法]：  private constructor <init>()V  228.  [文件]：  com/rwin/pub/BoxManager  [方法]：  public declared-synchronized connectBluetooth(Landroid/bluetooth/BluetoothDevice;)Z  229.  [文件]：  com/rwin/pub/BoxManager  [方法]：  public doBluetoothLogic()Z  230.  [文件]：  com/rwin/pub/BoxManager  [方法]：  public declared-synchronized getBluetoothConnectState()I  231.  [文件]：  com/rwin/pub/IDCardModule  [方法]：  private checkFile(Landroid/content/Context;Ljava/lang/String;Ljava/lang/String;)V  232.  [文件]：  com/rwin/pub/IDCardModule  [方法]：  private read\_gz()Ljava/lang/String;  233.  [文件]：  com/rwin/pub/IDCardModule  [方法]：  public read(Landroid/content/Context;)Ljava/lang/String;  234.  [文件]：  com/rwin/pub/IDCardModule  [方法]：  public readBarCode()Ljava/lang/String;  235.  [文件]：  com/rwin/pub/IDCardModule  [方法]：  writeBytesToFile(Ljava/lang/String;[B)V  236.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  private CheckCfgPrivate(Landroid/content/Context;)Z  237.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  private checkFile(Landroid/content/Context;Ljava/lang/String;Ljava/lang/String;)V  238.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  public static getBmpSubRect(Ljava/lang/String;Ljava/lang/String;FFFFI)I  239.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  private myXz(Landroid/content/Context;Ljava/lang/String;)V  240.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  private setParam(Landroid/content/Context;)V  241.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  private static testCV(Ljava/lang/String;)V  242.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  public CheckCfg(Landroid/content/ContextWrapper;)Z  243.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  public getBackInfo(Landroid/content/Context;Ljava/lang/String;)Ljava/lang/String;  244.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  public getFrontInfo(Landroid/content/Context;Ljava/lang/String;)Ljava/lang/String;  245.  [文件]：  com/rwin/pub/IDCardImage  [方法]：  public getFrontInfo\_old(Landroid/content/Context;Ljava/lang/String;)Ljava/lang/String;  246.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  private addrn2Str(Ljava/lang/String;ILjava/lang/StringBuilder;)V  247.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  private checkPrintStr(Ljava/lang/String;)Ljava/lang/String;  248.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  private split(Ljava/lang/String;Ljava/util/List;)V  249.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  public getStatus()I  250.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  public isHavePaper()Z  251.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  public declared-synchronized printBitMap(Landroid/graphics/Bitmap;)I  252.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  public declared-synchronized printFormatInfo(ILjava/lang/String;)I  253.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  public declared-synchronized printString(ILjava/lang/String;)I  254.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  public printTest(I)I  255.  [文件]：  com/rwin/pub/RenWPrinter  [方法]：  public declared-synchronized prtbuf\_print()I  256.  [文件]：  com/rwin/pub/psamRWCardBox  [方法]：  private checkAppKey([B)I  257.  [文件]：  com/rwin/pub/psamRWCardBox  [方法]：  private checkMasterKey([B)I  258.  [文件]：  com/rwin/pub/psamRWCardBox  [方法]：  public changePinCode([BB[BB[BB[B)B  259.  [文件]：  com/rwin/pub/psamRWCardBox  [方法]：  public checkPinCode([BB[BB[B)B  260.  [文件]：  com/rwin/pub/psamRWCardBox  [方法]：  public getDesData([BBB[BB[B)B  261.  [文件]：  com/rwin/pub/psamRWCardBox  [方法]：  public readPsamCardId(B[B[B[B)B  262.  [文件]：  com/rwin/pub/psamRWCardBox  [方法]：  public requestAndWaitBox(Ljava/lang/String;[B[BILjava/lang/String;I)Z  263.  [文件]：  com/rwin/pub/psamRWCardBox  [方法]：  public sendAndRecvBox(Ljava/lang/String;I[B[BII)I  264.  [文件]：  com/sunrise/b  [方法]：  private a(Lcom/sunrise/reader/ReaderServerInfo;)[B  265.  [文件]：  com/sunrise/b  [方法]：  private e()Lcom/sunrise/u/a;  266.  [文件]：  com/sunrise/b  [方法]：  public a(Landroid/nfc/Tag;)Z  267.  [文件]：  com/sunrise/x/c  [方法]：  public run()V  268.  [文件]：  com/sunrise/OTGAndNFCClient  [方法]：  private closedReader()V  269.  [文件]：  com/sunrise/OTGAndNFCClient  [方法]：  private readCard(J)Ljava/lang/String;  270.  [文件]：  com/sunrise/OTGAndNFCClient  [方法]：  public cloudReadCert(Ljava/lang/String;Ljava/util/List;ILandroid/nfc/Tag;Ljava/lang/String;Ljava/lang/String;)Ljava/util/Map;  271.  [文件]：  com/sunrise/OTGAndNFCClient  [方法]：  public getReaderInfo()Ljava/util/Map;  272.  [文件]：  com/sunrise/OTGAndNFCClient  [方法]：  public idInfo(Lcom/sunrise/icardreader/model/IdentityCardZ;)V  273.  [文件]：  com/sunrise/b$2  [方法]：  public run()V  274.  [文件]：  com/sunrise/BtReaderClient$1  [方法]：  public idInfo(Lcom/sunrise/icardreader/model/IdentityCardZ;)V  275.  [文件]：  com/sunrise/reader/pos/YifengPosReader$1  [方法]：  protected varargs doInBackground([Ljava/lang/Object;)Ljava/lang/Boolean;  276.  [文件]：  com/sunrise/reader/pos/JBPosNFC  [方法]：  public findIDCard(Landroid/nfc/NfcAdapter$ReaderCallback;)Z  277.  [文件]：  com/sunrise/reader/pos/JBPosNFC  [方法]：  public icCardTransmitApdu([B)[B  278.  [文件]：  com/sunrise/reader/pos/JBPosNFC  [方法]：  public transceive([B)[B  279.  [文件]：  com/sunrise/reader/pos/JBPosNFC$1  [方法]：  public onError(ILjava/lang/String;)V  280.  [文件]：  com/sunrise/reader/pos/JBPosNFC$1  [方法]：  public onSuccess(I)V  281.  [文件]：  com/sunrise/reader/pos/BaifuPosReader  [方法]：  public findIDCard(Landroid/nfc/NfcAdapter$ReaderCallback;)Z  282.  [文件]：  com/sunrise/reader/pos/BaifuPosReader  [方法]：  public init()V  283.  [文件]：  com/sunrise/reader/pos/BaifuPosReader$1  [方法]：  protected varargs doInBackground([Ljava/lang/Object;)Ljava/lang/Boolean;  284.  [文件]：  com/sunrise/reader/pos/YifengPosReader  [方法]：  public transceive([B)[B  285.  [文件]：  com/sunrise/reader/pos/YifengPosReader  [方法]：  public unBind()V  286.  [文件]：  com/sunrise/reader/ReadIDCardDriver$1  [方法]：  public run()V  287.  [文件]：  com/sunrise/reader/m  [方法]：  private a(Landroid/hardware/usb/UsbDevice;)Z  288.  [文件]：  com/sunrise/reader/m  [方法]：  public a(Lcom/sunrise/u/a;)Lcom/sunrise/u/a;  289.  [文件]：  com/sunrise/reader/m  [方法]：  public c()Z  290.  [文件]：  com/sunrise/reader/m  [方法]：  public d()[B  291.  [文件]：  com/sunrise/reader/m  [方法]：  public send\_cmd\_to\_reader([B)[B  292.  [文件]：  com/sunrise/reader/ReaderManagerService  [方法]：  private registerReceiver()V  293.  [文件]：  com/sunrise/reader/ReaderManagerService  [方法]：  public static stopServer()V  294.  [文件]：  com/sunrise/reader/ReaderManagerService  [方法]：  public quit()V  295.  [文件]：  com/sunrise/reader/ReaderManagerService  [方法]：  public saveServerIndex(I)V  296.  [文件]：  com/sunrise/reader/ReaderManagerService  [方法]：  public upload(Ljava/io/File;)I  297.  [文件]：  com/sunrise/reader/serialport/SerialPortReader  [方法]：  public authId(Lcom/sunrise/u/a;)Lcom/sunrise/u/a;  298.  [文件]：  com/sunrise/reader/serialport/SerialPortReader  [方法]：  public cardPowerOn()Lcom/sunrise/u/a;  299.  [文件]：  com/sunrise/reader/serialport/SerialPortReader  [方法]：  public open()I  300.  [文件]：  com/sunrise/reader/serialport/SerialPortReader  [方法]：  public openId()Lcom/sunrise/u/a;  301.  [文件]：  com/sunrise/reader/serialport/SerialPortReader  [方法]：  public readInfo(Lcom/sunrise/u/a;)Lcom/sunrise/u/a;  302.  [文件]：  com/sunrise/reader/serialport/SerialPortReader  [方法]：  public transmitAPDU(Lcom/sunrise/u/a;)Lcom/sunrise/u/a;  303.  [文件]：  com/sunrise/reader/f  [方法]：  public a(Lcom/sunrise/reader/ManagerInfo;)I  304.  [文件]：  com/sunrise/reader/f  [方法]：  public a(Lcom/sunrise/reader/ReaderServerInfo;)Lcom/sunrise/reader/f;  305.  [文件]：  com/sunrise/reader/f  [方法]：  public b()V  306.  [文件]：  com/sunrise/reader/o  [方法]：  public run()V  307.  [文件]：  com/sunrise/reader/d  [方法]：  public run()V  308.  [文件]：  com/sunrise/reader/b  [方法]：  public constructor <init>(Lcom/sunrise/reader/a;Landroid/bluetooth/BluetoothDevice;)V  309.  [文件]：  com/sunrise/reader/b  [方法]：  public a()V  310.  [文件]：  com/sunrise/reader/b  [方法]：  public run()V  311.  [文件]：  com/sunrise/reader/s  [方法]：  public run()V  312.  [文件]：  com/sunrise/reader/c$1  [方法]：  public run()V  313.  [文件]：  com/sunrise/reader/p  [方法]：  public run()V  314.  [文件]：  com/sunrise/reader/l  [方法]：  public static a(Ljava/lang/String;Ljava/lang/String;)V  315.  [文件]：  com/sunrise/reader/l  [方法]：  public static a(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Exception;)V  316.  [文件]：  com/sunrise/reader/a  [方法]：  private c()V  317.  [文件]：  com/sunrise/reader/a  [方法]：  public a(Ljava/lang/String;)I  318.  [文件]：  com/sunrise/reader/a  [方法]：  a(Lcom/sunrise/u/a;)Lcom/sunrise/u/a;  319.  [文件]：  com/sunrise/reader/a  [方法]：  public declared-synchronized send\_cmd\_to\_reader([B)[B  320.  [文件]：  com/sunrise/reader/r  [方法]：  public static b(Ljava/lang/String;)V  321.  [文件]：  com/sunrise/reader/q  [方法]：  public a(Lcom/sunrise/r/d;)I  322.  [文件]：  com/sunrise/reader/n  [方法]：  private a(Lcom/sunrise/reader/f;)I  323.  [文件]：  com/sunrise/reader/n  [方法]：  private a(Lcom/sunrise/u/a;)V  324.  [文件]：  com/sunrise/reader/n  [方法]：  private a([BLjava/lang/String;I)[B  325.  [文件]：  com/sunrise/reader/n  [方法]：  private m()I  326.  [文件]：  com/sunrise/reader/n  [方法]：  private n()V  327.  [文件]：  com/sunrise/reader/n  [方法]：  public g()Z  328.  [文件]：  com/sunrise/reader/n  [方法]：  public i()[B  329.  [文件]：  com/sunrise/reader/n  [方法]：  public j()Ljava/util/Map;  330.  [文件]：  com/sunrise/reader/ReadIDCardDriver  [方法]：  private driverReaderId()I  331.  [文件]：  com/sunrise/reader/ReadIDCardDriver  [方法]：  public getReaderName()Ljava/lang/String;  332.  [文件]：  com/sunrise/reader/ReadIDCardDriver  [方法]：  public openReader()I  333.  [文件]：  com/sunrise/reader/ReadIDCardDriver  [方法]：  public openReader(Ljava/lang/String;)I  334.  [文件]：  com/sunrise/reader/c  [方法]：  private a(Lcom/sunrise/u/a;)V  335.  [文件]：  com/sunrise/reader/c  [方法]：  private a([BLjava/lang/String;I)[B  336.  [文件]：  com/sunrise/reader/c  [方法]：  private j()I  337.  [文件]：  com/sunrise/reader/c  [方法]：  public a(Ljava/lang/String;)I  338.  [文件]：  com/sunrise/reader/c  [方法]：  public a()V  339.  [文件]：  com/sunrise/reader/c  [方法]：  public c()Ljava/lang/String;  340.  [文件]：  com/sunrise/reader/c  [方法]：  public g()[B  341.  [文件]：  com/sunrise/reader/c  [方法]：  public h()Ljava/util/Map;  342.  [文件]：  com/sunrise/reader/u  [方法]：  public static a(Landroid/content/Context;)Ljava/lang/String;  343.  [文件]：  com/sunrise/reader/u  [方法]：  public static a(ILcom/sunrise/reader/ManagerInfo;Ljava/lang/String;ILjava/lang/String;)V  344.  [文件]：  com/sunrise/m/a  [方法]：  private static a(Ljava/lang/Class;Landroid/app/Fragment;Ljava/lang/String;I)V  345.  [文件]：  com/sunrise/m/a  [方法]：  private static b(Ljava/lang/Class;Landroid/app/Fragment;Ljava/lang/Exception;)V  346.  [文件]：  com/sunrise/BtReaderClient  [方法]：  private closedReader()V  347.  [文件]：  com/sunrise/BtReaderClient  [方法]：  private readCard(J)Ljava/lang/String;  348.  [文件]：  com/sunrise/BtReaderClient  [方法]：  public cloudReadCert(Ljava/lang/String;Ljava/util/List;Ljava/lang/String;Ljava/lang/String;)Ljava/util/Map;  349.  [文件]：  com/sunrise/BtReaderClient  [方法]：  public getReaderInfo()Ljava/util/Map;  350.  [文件]：  com/sdses/Files  [方法]：  public WriteByteToFile(Ljava/lang/String;[BIIZ)V  351.  [文件]：  com/sdses/Files  [方法]：  public WriteStringToFile(Ljava/lang/String;Ljava/lang/String;Z)V  352.  [文件]：  com/sdses/Communication$ReadWriteThread  [方法]：  public read([B)I  353.  [文件]：  com/sdses/Communication  [方法]：  public constructor <init>(Ljava/lang/String;)V  354.  [文件]：  com/sdses/Communication  [方法]：  public ClearBuff()V  355.  [文件]：  com/sdses/Communication  [方法]：  public ReceiveMessage(I)Ljava/util/HashMap;  356.  [文件]：  com/sdses/Communication  [方法]：  public ReceiveMessage(II)Ljava/util/HashMap;  357.  [文件]：  com/sdses/BtReaderClient$1  [方法]：  public onReceive(Landroid/content/Context;Landroid/content/Intent;)V  358.  [文件]：  com/sdses/BtReaderClient  [方法]：  public constructor <init>(Landroid/app/Activity;)V  359.  [文件]：  com/sdses/BtReaderClient  [方法]：  private GetDataFromHash(Ljava/util/HashMap;)[B  360.  [文件]：  com/sdses/BtReaderClient  [方法]：  public static GetSID(JJ)[B  361.  [文件]：  com/sdses/BtReaderClient  [方法]：  private sendCmdChinaTelecom(I[BIII)I  362.  [文件]：  com/sdses/BtReaderClient  [方法]：  private sendCmdChinaTelecom2(I[BIII)I  363.  [文件]：  com/sdses/BtReaderClient  [方法]：  private updateKey(Ljava/lang/String;)Ljava/util/HashMap;  364.  [文件]：  com/sdses/BtReaderClient  [方法]：  public GetCardInfoBytes()[B  365.  [文件]：  com/sdses/BtReaderClient  [方法]：  public GetEndDate([B)Ljava/lang/String;  366.  [文件]：  com/sdses/BtReaderClient  [方法]：  public GetPic(Ljava/lang/String;Ljava/lang/String;)I  367.  [文件]：  com/sdses/BtReaderClient  [方法]：  public createTotalinfoXML(Ljava/lang/String;Ljava/lang/String;)Ljava/util/HashMap;  368.  [文件]：  com/sdses/BtReaderClient  [方法]：  public readBtType([B)I  369.  [文件]：  com/sdses/BtReaderClient  [方法]：  public readCert()Ljava/util/HashMap;  370.  [文件]：  com/sdses/BtReaderClient  [方法]：  public readDevName([B)I  371.  [文件]：  com/sdses/BtReaderClient  [方法]：  public readDevVersion([B)I  372.  [文件]：  com/sdses/BtReaderClient  [方法]：  public readHardwareVersion([B)I  373.  [文件]：  com/sdses/BtReaderClient  [方法]：  public readId2InitData()[B  374.  [文件]：  com/sdses/BtReaderClient  [方法]：  public readId2InitDataWithFp([B)I  375.  [文件]：  com/sdses/BtReaderClient  [方法]：  public readSamID([B)I  376.  [文件]：  com/sdses/BtReaderClient  [方法]：  public readSoftVersion([B)I  377.  [文件]：  com/sdses/BtReaderClient  [方法]：  public setFpLabel(Ljava/lang/String;)I  378.  [文件]：  com/ist/usb/BoxIDCardModule  [方法]：  private checkFile(Landroid/content/Context;Ljava/lang/String;Ljava/lang/String;)V  379.  [文件]：  com/ist/usb/BoxIDCardModule  [方法]：  public read(Landroid/content/Context;)Ljava/lang/String;  380.  [文件]：  com/ist/bluetooth/BluetoothControler  [方法]：  public static declared-synchronized reConnect()Z  381.  [文件]：  com/ist/bluetooth/BluetoothControler\_java  [方法]：  public static declared-synchronized connect(Landroid/bluetooth/BluetoothDevice;)Z  382.  [文件]：  com/ist/bluetooth/BluetoothControler\_java  [方法]：  public static declared-synchronized reConnect()Z  383.  [文件]：  cn/cloudwalk/libproject/net/ApacheHttpUtil  [方法]：  public static get(Ljava/lang/String;Ljava/util/Map;)Ljava/lang/String;  384.  [文件]：  cn/cloudwalk/libproject/net/ApacheHttpUtil  [方法]：  public static post(Ljava/lang/String;Ljava/util/List;)Ljava/lang/String;  385.  [文件]：  cn/cloudwalk/libproject/net/HttpManager$1  [方法]：  protected onPostExecute(Ljava/lang/String;)V  386.  [文件]：  cn/cloudwalk/libproject/LiveActivity  [方法]：  protected onCreate(Landroid/os/Bundle;)V  387.  [文件]：  cn/cloudwalk/libproject/camera/CameraConfigurationManager  [方法]：  private getOptimalPreviewSize(Ljava/util/List;II)Landroid/hardware/Camera$Size;  388.  [文件]：  cn/cloudwalk/libproject/camera/CameraConfigurationManager  [方法]：  public setCameraParametersForPreviewCallBack(Landroid/hardware/Camera;III)I  389.  [文件]：  cn/cloudwalk/libproject/camera/CameraConfigurationManager  [方法]：  public setDesiredCameraParameters(Landroid/hardware/Camera;I)V  390.  [文件]：  cn/cloudwalk/libproject/camera/CameraPreview  [方法]：  public onPreviewFrame([BLandroid/hardware/Camera;)V  391.  [文件]：  cn/cloudwalk/libproject/view/RoundProgressBar  [方法]：  protected onDraw(Landroid/graphics/Canvas;)V  392.  [文件]：  cn/cloudwalk/libproject/view/CustomViewPager  [方法]：  public constructor <init>(Landroid/content/Context;Landroid/util/AttributeSet;)V  393.  [文件]：  cn/cloudwalk/libproject/BestFaceActivity$MainHandler  [方法]：  public handleMessage(Landroid/os/Message;)V  394.  [文件]：  cn/cloudwalk/libproject/util/TestUtil  [方法]：  public static time1sCount(Ljava/lang/String;)V  395.  [文件]：  cn/cloudwalk/libproject/util/TestUtil  [方法]：  public static time1sCount2(Ljava/lang/String;)V  396.  [文件]：  cn/cloudwalk/libproject/util/TestUtil  [方法]：  public static timeCount()V  397.  [文件]：  cn/cloudwalk/libproject/util/TestUtil  [方法]：  public static timeEnd(Ljava/lang/String;)V  398.  [文件]：  cn/cloudwalk/libproject/util/FileUtil  [方法]：  public static copyFile(Ljava/lang/String;Ljava/lang/String;)V  399.  [文件]：  cn/cloudwalk/libproject/util/FileUtil  [方法]：  public static copyRawFileToSdcard(Ljava/lang/String;Landroid/content/res/AssetManager;Ljava/lang/String;)V  400.  [文件]：  cn/cloudwalk/libproject/util/FileUtil  [方法]：  public static createModelFile(Ljava/lang/String;Ljava/lang/String;Landroid/content/res/AssetManager;)V  401.  [文件]：  cn/cloudwalk/libproject/util/FileUtil  [方法]：  public static createModelFileAll(Ljava/lang/String;Landroid/content/res/AssetManager;)V  402.  [文件]：  cn/cloudwalk/libproject/util/FileUtil  [方法]：  public static readRawFileToByteArray(Ljava/lang/String;Landroid/content/res/AssetManager;)[B  403.  [文件]：  cn/cloudwalk/libproject/util/FileUtil  [方法]：  public static readRawFileToString(Ljava/lang/String;Landroid/content/res/AssetManager;)Ljava/lang/String;  404.  [文件]：  cn/cloudwalk/libproject/util/Util  [方法]：  public static final MD5(Ljava/lang/String;)Ljava/lang/String;  405.  [文件]：  cn/cloudwalk/libproject/util/Util  [方法]：  public static getFilePath(Ljava/lang/String;)Ljava/lang/String;  406.  [文件]：  cn/cloudwalk/libproject/util/Util  [方法]：  public static getStatusBarHeight(Landroid/content/Context;)I  407.  [文件]：  cn/cloudwalk/libproject/util/ThumbnailUtil  [方法]：  public static getRealPathFromURI(Landroid/net/Uri;Landroid/content/Context;)[Ljava/lang/String;  408.  [文件]：  cn/cloudwalk/libproject/util/ScreenUtils  [方法]：  public static getStatusHeight(Landroid/content/Context;)I  409.  [文件]：  cn/cloudwalk/CloudwalkSDK  [方法]：  private cwClipFaceBitmap(Landroid/graphics/Bitmap;Lcn/cloudwalk/jni/FaceLivingImg;)Landroid/graphics/Bitmap;  410.  [文件]：  cn/cloudwalk/CloudwalkSDK  [方法]：  private cwGetIDFaceImage(Landroid/graphics/Bitmap;I)Landroid/graphics/Bitmap;  411.  [文件]：  cn/cloudwalk/CloudwalkSDK  [方法]：  private cwStop()I  412.  [文件]：  cn/cloudwalk/CloudwalkSDK  [方法]：  private processVideoFrame(Lcn/cloudwalk/CloudwalkSDK$Frame;)V  413.  [文件]：  cn/cloudwalk/CloudwalkSDK  [方法]：  public cwGetClipedBestFace()[B  414.  [文件]：  cn/cloudwalk/CloudwalkSDK  [方法]：  public cwGetNextFace()[B  415.  [文件]：  cn/cloudwalk/CloudwalkSDK  [方法]：  public cwGetOriBestFace()[B  416.  [文件]：  cn/cloudwalk/CloudwalkSDK  [方法]：  public cwInit(Landroid/content/Context;Ljava/lang/String;)I  417.  [文件]：  cn/cloudwalk/CloudwalkSDK  [方法]：  public cwPushFrame([BIIIII)V  418.  [文件]：  wintone/idcard/android/IDCardCfg  [方法]：  public String2Int(Ljava/lang/String;)I  419.  [文件]：  wintone/idcard/android/IDCardCfg  [方法]：  public onCreate(Landroid/os/Bundle;)V  420.  [文件]：  wintone/idcard/android/IDCardBean$2  [方法]：  public onServiceConnected(Landroid/content/ComponentName;Landroid/os/IBinder;)V  421.  [文件]：  wintone/idcard/android/RecogService  [方法]：  private String2Int(Ljava/lang/String;)I  422.  [文件]：  wintone/idcard/android/RecogService  [方法]：  public onCreate()V  423.  [文件]：  wintone/idcard/android/RecogService  [方法]：  public readInitFileString(Ljava/lang/String;)Ljava/lang/String;  424.  [文件]：  wintone/idcard/android/RecogService$recogBinder  [方法]：  public IDCardAuthAndInit(Lwintone/idcard/android/RecogParameterMessage;)I  425.  [文件]：  wintone/idcard/android/RecogService$recogBinder  [方法]：  public IDCardCutNoLineationImage(Lwintone/idcard/android/RecogParameterMessage;)V  426.  [文件]：  wintone/idcard/android/RecogService$recogBinder  [方法]：  public IDCardLoadAndRecogMRZ(Lwintone/idcard/android/RecogParameterMessage;)V  427.  [文件]：  wintone/idcard/android/RecogService$recogBinder  [方法]：  public IDCardLoadNoLineationImage(Lwintone/idcard/android/RecogParameterMessage;)V  428.  [文件]：  wintone/idcard/android/RecogService$recogBinder  [方法]：  public IDCardRecognitionImage(Lwintone/idcard/android/RecogParameterMessage;)V  429.  [文件]：  wintone/idcard/android/AuthService  [方法]：  public onCreate()V  430.  [文件]：  wintone/idcard/android/IDCardBean  [方法]：  private String2Int(Ljava/lang/String;)I  431.  [文件]：  wintone/idcard/android/IDCardBean  [方法]：  public ReturnResultToActivity(Lwintone/idcard/android/ResultMessage;)V  432.  [文件]：  wintone/idcard/android/IDCardBean  [方法]：  public onCreate(Landroid/os/Bundle;)V  433.  [文件]：  wintone/idcard/android/IDCardBean  [方法]：  public startRecog()V  434.  [文件]：  android\_serialport\_api/SerialPort  [方法]：  public constructor <init>(Ljava/io/File;II)V  435.  [文件]：  android\_serialport\_api/SerialPort  [方法]：  public sendCmd([B)[B |
| **解决方案** | 开发者自查：关闭调试日志函数调用，或者确保日志的输出使用了正确的级别，涉及敏感数据的日志信息在发布版本中被关闭。 |

### 数据库注入漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App应用的数据库是否存在sql注入漏洞。 |
| **危险等级** | 高 |
| **危害** | 由于Content provider组件读写权限设置不当，并且未对sql查询语句的字段参数作过滤判断，app本地数据库可能被注入攻击。这种风险可能导致存储的敏感数据信息被查询泄露，例如账户名，密码等，或者产生查询异常导致应用崩溃。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### AES/DES加密方法不安全使用漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App程序中使用AES/DES加密算法时是否使用了不安全的加密模式。 |
| **危险等级** | 低 |
| **危害** | AES/DES是android程序中常用的两种对称加密算法，其工作模式有ECB、CBC、CFB和OFB。当其使用ECB或OFB工作模式时，加密数据可能被选择明文攻击CPA破解。加密方法失效后可能导致客户端隐私数据泄露，加密文件破解，传输数据被获取，中间人攻击等后果，造成用户敏感信息被窃取。 |
| **测评结果** | 存在漏洞(发现6处) |
| **测评结果描述** | 该App程序中的加密算法使用了不安全的加密模式。 |
| **测评详细信息** | 1.  [文件]：  com/wintone/cipher/AES  [方法]：  public Encrypt([B[B)[B  2.  [文件]：  com/wintone/cipher/AES  [方法]：  public decrypt([B[B)[B  3.  [文件]：  com/wintone/cipher/AESofSUN  [方法]：  public Encrypt([B[B)[B  4.  [文件]：  com/wintone/cipher/AESofSUN  [方法]：  public decrypt([B[B)[B  5.  [文件]：  com/sdses/Util  [方法]：  public static desDecrypt([B[B[B)V  6.  [文件]：  com/sdses/Util  [方法]：  public static desEncrypt([B[B)[B |
| **解决方案** | 开发者自查：使用AES/DES加密算法时应显示设定工作模式为CBC或CFB模式。 |

### RSA加密算法不安全使用漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在RSA加密算法不安全使用的漏洞。 |
| **危险等级** | 中 |
| **危害** | RSA算法是最为典型的非对称加密算法，也是当今应用范围最为广泛的非对称加密算法，也是第一个能用于数据加密也能用于数字签名的算法。使用RSA加密算法时，应注意以下两点：1.密钥长度过短，会导致密钥被破解，通常小于512bit的密钥即存在破解的风险；2.加密算法没有使用正确的工作模式和填充方式，容易导致部分加密数据被破解或者遭到选择明文攻击（CPA）。RSA加密算法的不安全使用，可能导致客户端隐私数据泄露，加密文件破解，传输数据被获取，中间人攻击等后果，造成用户敏感信息被窃取，甚至造成财产损失。 |
| **测评结果** | 存在漏洞(发现4处) |
| **测评结果描述** | 该App中存在不安全的RSA加密算法使用漏洞。 |
| **测评详细信息** | 1.  [文件]：  com/wintone/cipher/RSA  [方法]：  public Decrypt([B)[B  2.  [文件]：  com/wintone/cipher/RSA  [方法]：  public Encrypt([B)[B  3.  [文件]：  com/wintone/cipher/RSA  [方法]：  public Sign([B)[B  4.  [文件]：  com/wintone/cipher/RSA  [方法]：  public Verify([B)[B |
| **解决方案** | 开发者自查：使用RSA加密算法时，密钥长度建议设置为2048bit，同时分别设置工作模式为ECB，填充模式为OAEPWithSHA256AndMGF1Padding。以下为修复代码示例：  1.KeyPairGenerator DemoKey=KeyPairGenerator.getInstance("RSA");  DemoKey.initialize(2048);  2.Cipher DemoCipher = Cipher.getInstance("RSA/ECB/OAEPWithSHA256AndMGF1Padding");  DemoCipher.init(Cipher.ENCRYPT\_MODE, keyPrivate); |

### 密钥硬编码漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在密钥硬编码漏洞。 |
| **危险等级** | 高 |
| **危害** | 密钥硬编码是指在代码中直接将加密算法的密钥设置为一个固定值。通常加密算法本身都是公开的，而加密内容的保密则主要是依赖于加密密钥。如果密钥泄露，根据加密算法和加密后的密文，很容易得到加密前的明文。而密钥硬编码在代码中，通过反编译攻击者可以直接查看密钥内容，整个加密算法将形同虚设。密钥硬编码，可直接造成加密数据被破解，客户端与服务器之间的通信内容被破解，导致应用内的加密文件被破解，或是用户的敏感信息泄露。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用中不存在密钥硬编码漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 动态调试攻击风险

|  |  |
| --- | --- |
| **测评目的** | 检测客户端App运行时是否面临C层动态调试的风险。 |
| **危险等级** | 高 |
| **危害** | 如果App存在C层代码动态调试的风险，攻击者可以利用GDB、IDA、Ptrace等调试器跟踪运行的目标程序，查看、修改内存中的代码和数据，甚至分析篡改程序的业务逻辑，对客户关键数据或者服务器进行恶意攻击，例如修改客户端业务操作的数据，比如转账账号、金额等，导致用户的损失。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Webview远程调试风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序是否存在Webview远程调试风险。 |
| **危险等级** | 中 |
| **危害** | Android应用可在WebView中直接实现对js代码的远程调试。在4.4版本以上的Android系统上可通过将WebView类静态方法 setWebContentsDebuggingEnabled设置为true，然后使用Chrome浏览器的开发工具inspect在Android应用中直接调试WebView。开启Webview的远程调试功能，可能会被非法使用者直接利用，获取js源代码，从而可能造成功能逻辑泄露；如果js被篡改，可能被植入钓鱼页面或者恶意代码，造成用户的敏感信息泄露。 |
| **测评结果** | 存在风险(发现1处) |
| **测评结果描述** | 该App存在Webview远程调试风险。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private initWebView()V |
| **解决方案** | 开发者自查：  如果使用的是4.4版本或更高版本的Android系统，在应用发布之前，确定WebView类中的静态方法setWebContentsDebuggingEnabled为默认设置或者显示设置为false。 |

### 应用数据任意备份风险

|  |  |
| --- | --- |
| **测评目的** | 检测App是否存在应用数据被任意备份的风险。 |
| **危险等级** | 中 |
| **危害** | Android 2.1以上的系统可为App提供应用程序数据的备份和恢复功能，该由AndroidMainfest.xml文件中的allowBackup属性值控制，其默认值为true。当该属性没有显式设置为false时，攻击者可通过adb backup和adb restore对App的应用数据进行备份和恢复，从而可能获取明文存储的用户敏感信息，如用户的密码、证件号、手机号、交易密码、身份令牌、服务器通信记录等。利用此类信息攻击者可伪造用户身份，盗取用户账户资产，或者直接对服务器发起攻击。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App中的应用数据不存在被外部调用备份的风险。 |
| **测评详细信息** | android:allowBackup="false" |
| **解决方案** |  |

### 敏感函数调用风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序中是否调用了包含敏感行为的函数。 |
| **危险等级** | 低 |
| **危害** | 敏感行为包括发送、拦截短信，读取、修改通讯录、通话记录，拨打电话，发送地理位置，使用摄像头，访问浏览器历史记录等。函数调用这些敏感行为，可能导致用户隐私数据泄露，钓鱼扣费等风险。 |
| **测评结果** | 存在风险(发现15处) |
| **测评结果描述** | 该App在运行过程中将会调用敏感函数，存在发生以下敏感行为的风险。 |
| **测评详细信息** | 1.  [文件]：  com/ctsi/idcertification/CloudReaderClient  [方法]：  private ReadCard(Lcom/ctsi/idcertification/entity/AuthInfo;I)V  [代码]：  Landroid/telephony/TelephonyManager;.getDeviceId - 获取设备信息  2.  [文件]：  com/ai/smartcrm/activity/CommonApplication  [方法]：  public init()V  [代码]：  Landroid/telephony/TelephonyManager;.getDeviceId - 获取设备信息  3.  [文件]：  com/ai/smartcrm/nfc/NFCActivity  [方法]：  private initData()V  [代码]：  Landroid/telephony/TelephonyManager;.getDeviceId - 获取设备信息  4.  [文件]：  com/sunrise/reader/u  [方法]：  public static a(Landroid/content/Context;)Ljava/lang/String;  [代码]：  Landroid/telephony/TelephonyManager;.getDeviceId - 获取设备信息  5.  [文件]：  com/sunrise/BtReaderClient  [方法]：  public constructor <init>(Landroid/content/Context;)V  [代码]：  Landroid/telephony/TelephonyManager;.getDeviceId - 获取设备信息  6.  [文件]：  wintone/idcard/android/RecogService  [方法]：  public onCreate()V  [代码]：  Landroid/telephony/TelephonyManager;.getDeviceId - 获取设备信息  7.  [文件]：  wintone/idcard/android/AuthService  [方法]：  public onCreate()V  [代码]：  Landroid/telephony/TelephonyManager;.getDeviceId - 获取设备信息  8.  [文件]：  wintone/idcard/android/IDCardBean  [方法]：  public onCreate(Landroid/os/Bundle;)V  [代码]：  Landroid/telephony/TelephonyManager;.getDeviceId - 获取设备信息  9.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private exec(ILjava/lang/String;)V  [代码]：  Landroid/telephony/TelephonyManager;.getSimSerialNumber - 获取SIM卡信息  10.  [文件]：  wintone/idcard/android/RecogService  [方法]：  public onCreate()V  [代码]：  Landroid/telephony/TelephonyManager;.getSimSerialNumber - 获取SIM卡信息  11.  [文件]：  wintone/idcard/android/AuthService  [方法]：  public onCreate()V  [代码]：  Landroid/telephony/TelephonyManager;.getSimSerialNumber - 获取SIM卡信息  12.  [文件]：  wintone/idcard/android/IDCardBean  [方法]：  public onCreate(Landroid/os/Bundle;)V  [代码]：  Landroid/telephony/TelephonyManager;.getSimSerialNumber - 获取SIM卡信息  13.  [文件]：  org/opencv/android/JavaCameraView  [方法]：  protected initializeCamera(II)Z  [代码]：  Landroid/hardware/Camera;.setPreviewDisplay - 相机操作  14.  [文件]：  com/ai/smartcrm/camera/CameraManager  [方法]：  public openDriver(Landroid/view/SurfaceHolder;)V  [代码]：  Landroid/hardware/Camera;.setPreviewDisplay - 相机操作  15.  [文件]：  cn/cloudwalk/libproject/camera/CameraPreview  [方法]：  public showCameraPreview()V  [代码]：  Landroid/hardware/Camera;.setPreviewDisplay - 相机操作 |
| **解决方案** | 开发者自查：审核包含敏感行为的函数调用，确保其使用是必要且限制于授权用户的。 |

### 数据库文件任意读写漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在可被任意读写的数据库文件。 |
| **危险等级** | 中 |
| **危害** | database配置模式安全风险源于:创建数据库(Database)时没有正确的选取合适的创建模式(MO DE\_PRIVATE、MODE\_WORLD\_READABLE以及MODE\_WORLD\_WRITEABLE)进行权限控制，从而导致数据库(Database)内容被恶意读写，造成账户密码、身份信息、金融账户其他敏感信息的泄露， 甚至可能导致攻击者进一步实施恶意攻击。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该Apk程序不存在可被任意读写的数据库文件。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 全局可读写的内部文件漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App应用中是否存在内部文件，可被其他任意App读写。 |
| **危险等级** | 中 |
| **危害** | 为了实现不同软件之间的数据共享，设置内部文件为全局可读或全局可写，导致其他应用可以读取和修改该文件。如果此类文件包含了关键配置信息，账户信息数据等敏感信息，可能会被盗取或者恶意篡改，导致如程序无法运行，业务逻辑被修改等问题。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用不包含全局可读写内部文件。 |
| **测评详细信息** |  |
| **解决方案** |  |

### SharedPreferences数据全局可读写漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在SharedPreferences数据全局可读写漏洞。 |
| **危险等级** | 中 |
| **危害** | SharedPreferences作为Android系统的本地数据存储方式之一，可将应用数据以键值对（key-value）的存储形式永久保存于App应用中。当使用SharedPreferences方式在创建本地存储文件时，如果使用了MODE\_WORLD\_READABLE模式，或者使用了MODE\_WORLD\_WRITEABLE模式并且配置了“android:sharedUserId”属性值时，可能导致储存于SharedPreferences文件中的敏感信息被其他程序读写，导致应用内明文存储的个人身份信息、密码以及token等重要敏感信息泄露，或者存储的用户信息、历史数据被篡改，诱导用户误操作等。更为严重的是具备root权限的程序或用户可对所有应用程序通过任意模式（包括MODE\_PRIVATE）创建的的Shared Preferences文件进行读写操作。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App中不存在SharedPreferences数据可被全局读写的漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### SharedUserId属性设置漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在sharedUserId属性设置漏洞。 |
| **危险等级** | 中 |
| **危害** | SharedPreferences作为Android系统的本地数据存储方式之一，可将应用数据以键值对（key-value）的存储形式永久保存于App应用中。当使用SharedPreferences方式在创建本地存储文件时，如果使用了MODE\_WORLD\_READABLE模式，或者使用了MODE\_WORLD\_WRITEABLE模式并且配置了“android:sharedUserId”属性值时，可能导致储存于SharedPreferences文件中的敏感信息被其他程序读写，导致应用内明文存储的个人身份信息、密码以及token等重要敏感信息泄露，或者存储的用户信息、历史数据被篡改，诱导用户误操作等。更为严重的是具备root权限的程序或用户可对所有应用程序通过任意模式（包括MODE\_PRIVATE）创建的的Shared Preferences文件进行读写操作。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App中不存在sharedUserId属性设置漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Internal Storage数据全局可读写漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在Internal Storage数据全局可读写漏洞。 |
| **危险等级** | 中 |
| **危害** | Internal Storage作为Android系统的本地数据存储方式之一，可将应用数据直接存储于设备的内部存储器中。当使用Internal Storage方式在创建本地存储文件时，如果使用了MODE\_WORLD\_READABLE模式，或者使用了MODE\_WORLD\_WRITEABLE模式，或者配置了“android:sharedUserId”属性值时，可能导致储存于Internal Storage文件中的敏感信息被其他程序读写，导致应用内明文存储的个人身份信息、密码以及token等重要敏感信息泄露，或者存储的用户信息、历史数据被篡改，诱导用户误操作等。更为严重的是具备root权限的程序或用户可对所有应用程序通过任意模式（包括MODE\_PRIVATE）创建的Internal Storage文件进行读写操作。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App中不存在Internal Storage数据全局可读写的漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### getDir数据全局可读写漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在getDir数据全局可读写的漏洞 |
| **危险等级** | 中 |
| **危害** | Context.getDir（String name , int mode）是访问Andoid系统的Internal Storage的一个重要方式，用于在应用程序的数据文件夹下获取或者创建一个存放应用程序自定义文件的文件夹。当该函数的第二参数使用了如果使用了MODE\_WORLD\_READABLE模式，或者使用了MODE\_WORLD\_WRITEABLE模式，或者配置了“android:sharedUserId”属性值时，可能导致储存于该文件夹中的敏感信息被其他程序读写，导致应用内明文存储的个人身份信息、密码以及token等重要敏感信息泄露，或者存储的用户信息、历史数据被篡改，诱导用户误操作等。更为严重的是具备root权限的程序或用户可对所有应用程序通过任意模式（包括MODE\_PRIVATE）创建的文件夹进行读写操作。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App中不存在getDir数据全局可读写的漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### FFmpeg文件读取漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在FFmpeg文件读取漏洞。 |
| **危险等级** | 高 |
| **危害** | FFmpeg是一个使用广泛的多媒体框架，支持解码、编码、转码、复用、解复用、流媒体、过滤器和播放几乎任何格式的多媒体文件，目前有非常多的视音频软件或是视频网站、手机 APP 都采用了这个库。该漏洞利用了FFmpeg处理HLS（HTTP Live Streaming）播放列表的功能，在 AVI 文件中的 GAB2字幕块中嵌入了一个恶意构造的HLS文件，然后提供使用FFmpeg的目标站点进行转码，在解析的过程中该avi文件被当做一个 XBIN 的视频流来处理，再通过XBIN的编解码器根据构造的目标路径把站点本地的文件包含进来，最后通过下载转码后的视频文件来获取目标站点本地的文件内容 (例如:/etc/passwd文件内容)。FFmpeg中存在的该漏洞，不仅可以触发本地文件读取以获得服务器文件，如果客户端使用了有漏洞的FFmpeg库,同样能触发本地文件读取漏洞,这样通过一段视频,就能获得手机中的文件内容了。该漏洞可能导致服务器端以及应用内存储的个人身份信息、密码等重要敏感信息泄露。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用中不存在FFmpeg文件读取漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Java层动态调试风险

|  |  |
| --- | --- |
| **测评目的** | 检测java层调试功能是否被打开，java代码层是否面临被动态调试的风险。 |
| **危险等级** | 中 |
| **危害** | 客户端软件AndroidManifest.xml中的调试标记如果开启，可被Java调试工具例如jdb进行调试，获取和篡改用户敏感信息，甚至分析并且修改代码实现的业务逻辑，例如窃取用户密码，绕过验证码防护等。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该Apk中AndroidManifest.xml中的调试标记已被关闭，Java层无法被调试。 |
| **测评详细信息** | android:debuggable="false" |
| **解决方案** |  |

### 剪切板敏感信息泄露漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App是否存在剪切板敏感信息泄露的漏洞。 |
| **危险等级** | 中 |
| **危害** | Android剪切板在后台可以暂存数据，如果把隐私数据，如密码，存放在剪切板中是不安全的，因为任何的应用程序都可以访问剪切板中的数据，且可以进行任意修改。如果用户复制的是明文敏感数据，那么其它应用程序通过访问剪贴板就可以获取到该明文敏感数据了，甚至可以通过监听剪切板中的内容来获取信息。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App不存在剪切板敏感信息泄露的漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 内网测试信息残留漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测程序代码内部是否包含残留测试信息，例如内网URL地址等。 |
| **危险等级** | 低 |
| **危害** | 通过检测移动应用是否包含内网URL地址，来判断发布包中是否包含测试数据。残留的测试数据，可能会被盗取并恶意利用在正式服务器上进行攻击，攻击安全薄弱的测试服务器以获取服务器安全漏洞或者逻辑漏洞。 |
| **测评结果** | 存在漏洞(发现2处) |
| **测评结果描述** | 该App应用中存在内网URL地址，可能存在更多的测试数据残留。 若需要了解该App应用中更多的URL信息，可查看URL信息检测详细内容。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/activity/MainActivity  [代码]：  http://10.6.9.52:8089/BizHall/sale/index  2.  [文件]：  com/ai/smartcrm/common/UrlConstant  [代码]：  http://10.6.9.52:8089/BizHall/sale/index |
| **解决方案** | 开发者自查：建议开发者根据测评结果检测相关文件中是否包含更多的测试数据。 |

### 随机数不安全使用漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测应用中是否存在随机数可被猜解的漏洞。 |
| **危险等级** | 低 |
| **危害** | Android应用中通常使用SecureRandom类来生成随机数值，用于程序的逻辑功能或者加密算法。错误的使用方式可造成生成的随机数并非完全随机分布，且产生重复的"随机值"。当SecureRandom类使用相同的种子生成随机数时，生成的随机数也相同，这样可导致使用的随机数或加密算法被破解。 |
| **测评结果** | 存在漏洞(发现4处) |
| **测评结果描述** | 该App应用中存在错误使用SecureRandom类的漏洞。 |
| **测评详细信息** | 1.  [文件]：  com/wintone/cipher/AES  [方法]：  public Encrypt([B[B)[B  2.  [文件]：  com/wintone/cipher/AES  [方法]：  public decrypt([B[B)[B  3.  [文件]：  com/wintone/cipher/AESofSUN  [方法]：  public Encrypt([B[B)[B  4.  [文件]：  com/wintone/cipher/AESofSUN  [方法]：  public decrypt([B[B)[B |
| **解决方案** | 开发者自查：禁止在生成随机数之前调用setSeed()方法设置随机种子或调用SecureRandom类的构造函数SecureRandom(byte[] seed)，建议通过/dev/urandom或者/dev/random获取的熵值来初始化伪随机数生成器。 |

### 代码残留URL信息检测

|  |  |
| --- | --- |
| **测评目的** | 检测程序代码内部存在的URL地址信息。 |
| **危险等级** | 低 |
| **危害** | 在移动应用的程序代码内部，可能存在大量开发人员或其他工作人员无意识留下的信息内容。URL信息检测就是通过检测移动应用程序代码内部所存在的URL地址信息，尽可能呈现出应用中所有的URL信息，便于应用开发者查看并评估其安全性。移动应用发布包中的URL地址信息，可能会被盗取并恶意利用在正式服务器上进行攻击，攻击安全薄弱的测试服务器以获取服务器安全漏洞或者逻辑漏洞。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用中未包含URL地址信息。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 残留账户密码信息检测

|  |  |
| --- | --- |
| **测评目的** | 检测程序代码内部是否包含残留的账户、密码信息。 |
| **危险等级** | 低 |
| **危害** | 移动应用发布包中如果存在残留的账户、密码信息，可能会被盗取并恶意利用在正式服务器上进行攻击，例如账号重试，攻击安全薄弱的测试服务器以获取服务器安全漏洞或者逻辑漏洞。 |
| **测评结果** | 存在漏洞(发现3处) |
| **测评结果描述** | 该App应用中存在残留的账户、密码信息。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/decoding/Intents$WifiConnect  [代码]：  .field public static final PASSWORD:Ljava/lang/String; = PASSWORD  2.  [文件]：  com/ai/smartcrm/util/SFTPUtil  [代码]：  .field public static final password:Ljava/lang/String; = newcrm  3.  [文件]：  com/ai/smartcrm/util/SFTPUtil  [代码]：  .field public static final username:Ljava/lang/String; = wasadm |
| **解决方案** | 开发者自查：  1、核查所有残留的账户和密码信息，删除与业务无关的账户和密码。  2、尽量不要将与客户端业务相关的账户密码信息以硬编码的方式写在应用客户端中。 |

### 残留手机号信息检测

|  |  |
| --- | --- |
| **测评目的** | 检测程序代码内部是否包含残留手机号信息。 |
| **危险等级** | 低 |
| **危害** | 移动应用发布包中如果存在残留的手机号信息，可能会被盗取并恶意利用在正式服务器上进行攻击，攻击安全薄弱的测试服务器以获取服务器安全漏洞或者逻辑漏洞。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用中未包含残留的手机号信息。 |
| **测评详细信息** |  |
| **解决方案** |  |

## 通信数据传输安全

### HTTP传输数据风险

|  |  |
| --- | --- |
| **测评目的** | 检测app程序是否使用HTTPS协议对传输数据进行加密。 |
| **危险等级** | 低 |
| **危害** | 无线传输的数据能被第三方轻易截获，由于客户端与服务器之间的传输数据遵循通信协议指定的格式和内容类型，如果未使用加密措施，传输数据可被还原成网络层的数据包并进行解包分析，直接暴露用户的各种关键数据，例如用户名，密码等。加入了SSL（Secure Socket Layer）子层实现的HTTPS协议可确保数据在网络上加密传输，即使传输的数据被截获，也无法解密和还原。 |
| **测评结果** | 存在风险(发现19处) |
| **测评结果描述** | 该App应用中使用了未加密的HTTP协议进行数据传输。 |
| **测评详细信息** | 1.  [文件]：  com/ctsi/idcertification/CloudReaderClient  [代码]：  http://smz.crm.189.cn:4001/api/v1/auth  2.  [文件]：  com/ai/smartcrm/update/UpdateManager$2  [代码]：  http://crm3.yn.189.cn:9500/app/yncrm\_version.xml  3.  [文件]：  com/ai/smartcrm/activity/ListActivity$8  [代码]：  http://crm3.yn.189.cn:9500/crm/so/decodeIdcPic  4.  [文件]：  com/ai/smartcrm/activity/MainActivity  [代码]：  http://crm3.yn.189.cn:9500/portal-web/portal/login  5.  [文件]：  com/ai/smartcrm/activity/MainActivity  [代码]：  http://10.6.9.52:8089/BizHall/sale/index  6.  [文件]：  com/ai/smartcrm/activity/MainActivity  [代码]：  http://222.221.11.113/BizHall/interface/index?staffNumber=  7.  [文件]：  com/ai/smartcrm/activity/MainActivity  [代码]：  http://135.33.6.202/BizHall/interface/index?staffNumber=  8.  [文件]：  com/ai/smartcrm/activity/MainActivity  [代码]：  http://135.32.111.4:9500/portal-web/main/mainPage  9.  [文件]：  com/ai/smartcrm/activity/MainActivity$3  [代码]：  http://crm3.yn.189.cn:9500/portal-web/portal/login  10.  [文件]：  com/ai/smartcrm/activity/MainActivity$3  [代码]：  http://135.32.111.4:9500/portal-web/main/mainPage  11.  [文件]：  com/ai/smartcrm/common/UrlConstant  [代码]：  http://crm3.yn.189.cn:9500/crm/so/decodeIdcPic  12.  [文件]：  com/ai/smartcrm/common/UrlConstant  [代码]：  http://10.6.9.52:8089/BizHall/sale/index  13.  [文件]：  com/ai/smartcrm/common/UrlConstant  [代码]：  http://135.33.6.202/BizHall/interface/index  14.  [文件]：  com/ai/smartcrm/common/UrlConstant  [代码]：  http://135.32.111.4:9500/portal-web/main/mainPage  15.  [文件]：  com/ai/smartcrm/common/UrlConstant  [代码]：  http://222.221.11.113/BizHall/interface/index  16.  [文件]：  com/ai/smartcrm/common/UrlConstant  [代码]：  http://crm3.yn.189.cn:9500/portal-web/portal/login  17.  [文件]：  com/ai/smartcrm/common/Constant  [代码]：  http://crm3.yn.189.cn:9500/app/yncrm\_version.xml  18.  [文件]：  com/wintone/lisence/CallWebService  [代码]：  http://webservice.wintone.com/  19.  [文件]：  com/wintone/lisence/CallWebService  [代码]：  http://www.idreader.com.cn:8888/cxfServer\_A/CardAuth? |
| **解决方案** | 开发者自查：使用HTTPS协议对传输数据进行加密保护。 |

### HTTPS未校验服务器证书漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App在使用HTTPS协议传输数据时是否对服务器证书进行校验。 |
| **危险等级** | 中 |
| **危害** | 使用HTTPS协议时，客户端必须对服务器身份进行完整性校验，以验证服务器是真实合法的目标服务器。如果没有校验，客户端可能与仿冒的服务器建立通信链接，即“中间人攻击”。Android中默认的HTTPS证书验证机制不接受不可信的连接，因而是安全的，但Android允许开发者重定义证书验证方法：1）使用X509TrustManager类检查证书是否合法并且是否未过期；2）使用HostnameVerifier类检查证书中的主机名与使用该证书的服务器的主机名是否一致。重写的X509TrustManager，其中的checkServerTrusted()方法不对验证失败做任何处理，即不对证书进行正确校验结果，是导致“中间人攻击”的主要原因之一。当发生中间人攻击时，仿冒的中间人可以冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息，甚至可能对通信内容进行篡改。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用在使用HTTPS协议传输数据时已对服务器证书进行了校验。 |
| **测评详细信息** |  |
| **解决方案** |  |

### HTTPS未校验主机名漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App在使用HTTPS协议传输数据时是否对服务器主机名进行校验。 |
| **危险等级** | 中 |
| **危害** | 使用HTTPS协议时，客户端必须对服务器身份进行完整性校验，以验证服务器是真实合法的目标服务器。如果没有校验，客户端可能与仿冒的服务器建立通信链接，即“中间人攻击”。Android中默认的HTTPS证书验证机制不接受不可信的连接，因而是安全的，但Android允许开发者重定义证书验证方法：1）使用X509TrustManager类检查证书是否合法并且是否未过期；2）使用HostnameVerifier类检查证书中的主机名与使用该证书的服务器的主机名是否一致。重写的HostnameVerifier，其中的Verify()方法不对主机名验证失败做任何处理，即不对主机名进行正确校验，是导致“中间人攻击”的主要原因之一。当发生中间人攻击时，仿冒的中间人可以冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息，甚至可能对通信内容进行篡改。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App在使用HTTPS协议传输数据时已对服务器主机名进行了校验。 |
| **测评详细信息** |  |
| **解决方案** |  |

### HTTPS允许任意主机名漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App在使用HTTPS协议传输数据时是否允许任意服务器主机名。 |
| **危险等级** | 中 |
| **危害** | 使用HTTPS协议时，客户端必须对服务器身份进行完整性校验，以验证服务器是真实合法的目标服务器。如果没有校验，客户端可能与仿冒的服务器建立通信链接，即“中间人攻击”。Android中默认的HTTPS证书验证机制不接受不可信的连接，因而是安全的，但Android允许开发者重定义证书验证方法：1）使用X509TrustManager类检查证书是否合法并且是否未过期；2）使用HostnameVerifier类检查证书中的主机名与使用该证书的服务器的主机名是否一致。重写的HostnameVerifier，当被配置为接受任何服务器主机名时，等同不对主机名进行校验，是导致“中间人攻击”的主要原因之一。当发生中间人攻击时，仿冒的中间人可以冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息，甚至可能对通信内容进行篡改。 |
| **测评结果** | 存在漏洞(发现1处) |
| **测评结果描述** | 该App应用在使用HTTPS进行数据传输时允许任意服务器主机名。 |
| **测评详细信息** | 1.  [文件]：  cn/cloudwalk/libproject/net/ApacheHttpUtil  [方法]：  private static getNewHttpClient()Lorg/apache/http/client/HttpClient; |
| **解决方案** | 开发者自查：开发者在使用https时应对服务器证书进行校验时，禁止允许任意服务器主机名。  以下为修复代码示例：  使用  SSLSocketFactory sf = new MySSLSocketFactory(trustStore);  sf.setHostnameVerifier(SSLSocketFactory.STRICT\_HOSTNAME\_VERIFIER);  代替  SSLSocketFactory sf = new MySSLSocketFactory(trustStore);  sf.setHostnameVerifier(SSLSocketFactory.ALLOW\_ALL\_HOSTNAME\_VERIFIER); |

### Webview绕过证书校验漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App应用的webview组件是否在发现https网页证书错误后继续加载页面。 |
| **危险等级** | 中 |
| **危害** | 客户端的Webview组件访问使用HTTPS协议加密的url时，如果服务器证书校验错误，客户端应该拒绝继续加载页面。但如果重载WebView的onReceivedSslError()函数并在其中执行handler.proceed()，客户端可以绕过证书校验错误继续访问此非法URL。这样将会导致“中间人攻击”，攻击者冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用不存在webview组件绕过证书校验的漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### HTTP报文信息泄漏风险

|  |  |
| --- | --- |
| **测评目的** | 检测app程序是否存在HTTP报文信息泄漏风险。 |
| **危险等级** | 低 |
| **危害** | 无线传输的数据能被第三方轻易截获，由于客户端与服务器之间的传输数据遵循通信协议指定的格式和内容类型，如果未使用加密措施，传输数据可被还原成网络层的数据包并进行解包分析，直接暴露用户的各种关键数据，例如用户名，密码等。加入了SSL（Secure Socket Layer）子层实现的HTTPS协议可确保数据在网络上加密传输，即使传输的数据被截获，也无法解密和还原。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

## 身份认证安全

### 界面劫持风险

|  |  |
| --- | --- |
| **测评目的** | 检测客户端App的应用界面是否存在可被劫持的风险。 |
| **危险等级** | 中 |
| **危害** | 界面劫持是指当客户端程序调用一个应用界面时，被恶意的第三方程序探知，如果该界面组件是恶意程序预设的攻击对象，恶意程序立即启动自己的仿冒界面并覆盖在客户端程序界面之上。此时用户可能在无察觉的情况下将自己的账号、密码信息输入到仿冒的信息输入界面中，恶意程序再把这些数据返回到服务器中，完成钓鱼攻击。目前主要的界面劫持攻击通常发生在Android5.0以下的设备中。界面劫持风险将导致用户关键信息，例如账号、密码、银行卡等关键信息被窃取等风险。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 输入监听风险

|  |  |
| --- | --- |
| **测评目的** | 检测app程序在进行输入时是否存在输入被监听的风险。 |
| **危险等级** | 中 |
| **危害** | 应用程序中的敏感信息通常主要来源于使用者的直接输入，如果用户的输入数据被监听或者按键位置被记录，很可能导致用户的输入数据被获取，其中的账号、密码等隐私信息泄露。而Android系统的默认输入键盘中通常都面临数据监听的风险。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用中未使用系统默认输入键盘。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 截屏攻击风险

|  |  |
| --- | --- |
| **测评目的** | 检测App的界面是否可被截图或者录制的风险。 |
| **危险等级** | 中 |
| **危害** | 截屏攻击是指对App应用运行中的界面进行截图或者录制。截图攻击的主要对象是Android应用中的身份认证、登录界面和资金操作界面。而在Android5.0中新增了屏幕录制接口，无需特殊权限，使用系统API （MediaProjection）即可实现屏幕录制，并且攻击程序可以通过自定义的字符覆盖掉系统的录屏提示，诱导用户在不知情的情况下启动屏幕录制功能。当恶意程序获取到应用截图或者屏幕录像后，将其发送给攻击者，攻击者便能直接查看或者还原手机界面的操作情况，从而轻而易举获取用户QQ、微信等应用的用户名及密码，甚至银行客户端中输入的银行账号及支付密码，导致用户的资金损失。 |
| **测评结果** | 存在风险(发现11处) |
| **测评结果描述** | 该App的界面存在被截屏攻击的风险。 |
| **测评详细信息** | 未禁止截屏的activity  1  [文件]：  com.ai.smartcrm.activity.MainActivity  2  [文件]：  com.ai.smartcrm.nfc.NFCActivity  3  [文件]：  com.ai.smartcrm.scan.CaptureScannerActivity  4  [文件]：  com.ai.smartcrm.activity.WintoneCameraActivity  5  [文件]：  wintone.idcard.android.IDCardBean  6  [文件]：  com.ai.smartcrm.printer.PrintSettingActivity  7  [文件]：  com.ai.smartcrm.printer.PrintTextActivity  8  [文件]：  com.ai.smartcrm.activity.ListActivity  9  [文件]：  cn.cloudwalk.libproject.LiveResultActivity  10  [文件]：  cn.cloudwalk.libproject.LiveActivity  11  [文件]：  cn.cloudwalk.libproject.LiveStartActivity |
| **解决方案** | 开发者自查：开发者审查应用中显示或者输入关键信息的界面，在此类Activity创建时设置WindowManager.LayoutParams.FLAG\_SECURE属性，该属性能防止屏幕被截图和录制。以下为修复代码示例：  public class DemoActivity extends Activity {  @Override  public void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  getWindow().setFlags(LayoutParams.FLAG\_SECURE, LayoutParams.FLAG\_SECURE);  setContentView(R.layout.main);  }  } |

## 内部数据交互安全

### 动态注册Receiver风险

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在动态注册Receiver风险。 |
| **危险等级** | 中 |
| **危害** | BroadcastReceiver组件的注册方式可分为两种，一种是静态注册，即提前在AndroidManifest.xml文件中声明组件；另外一种是动态注册，即在代码中使用registerReceiver()方法注册BroadcastReceiver，只有当registerReceiver()的代码执行到了才进行注册，取消时则调用unregisterReceiver()方法。而容易被忽略的是registerReceiver()方法注册的是全局BroadcastReceiver，在其生命周期里是默认可导出的，如果没有指定权限访问控制，可以被任意外部应用访问，向其传递Intent来执行特定的功能。因此，动态注册的BroadcastReceive可能导致拒绝服务攻击、应用数据泄漏或是越权调用等风险。 |
| **测评结果** | 存在风险(发现10处) |
| **测评结果描述** | 该App中存在动态注册Receiver风险。 |
| **测评详细信息** | 1.  [文件]：  com/invs/Blt2  [方法]：  public scanDevice(Z)V  2.  [文件]：  com/invs/BtReaderClient  [方法]：  regRecv()V  3.  [文件]：  com/Routon/iDRCtLib/BtReaderClient  [方法]：  public connectBt(Ljava/lang/String;)Ljava/lang/Boolean;  4.  [文件]：  com/wch/wchusbdriver/CH34xAndroidDriver  [方法]：  public ResumeUsbList()I  5.  [文件]：  com/zkc/helper/printer/BlueToothService  [方法]：  public ScanDevice()V  6.  [文件]：  com/ai/smartcrm/activity/ListActivity  [方法]：  protected onCreate(Landroid/os/Bundle;)V  7.  [文件]：  com/YinanSoft/BTDevice/Sdtusbapi  [方法]：  public initUSB(Landroid/content/Context;)I  8.  [文件]：  com/yast/yadrly001/BtReaderClient  [方法]：  public connectBt(ILjava/lang/String;Ljava/lang/String;)I  9.  [文件]：  com/yast/yadrly001/BtReaderClient  [方法]：  public connectBt(Ljava/lang/String;)Z  10.  [文件]：  com/sdses/BtReaderClient  [方法]：  public constructor <init>(Landroid/app/Activity;)V |
| **解决方案** | 开发者自查：  1.开发者可使用LocalBroadcastManager来实现BroadcastReceiver动态注册，保证数据传递仅限于应用内。  以下为修复代码示例：  public static void sendLocalBroadcast(Intent intent) {  LocalBroadcastManager.getInstance(getInstance()).sendBroadcastSync(intent);  }  public static void registerLocalReceiver(BroadcastReceiver receiver, IntentFilter filter) {  LocalBroadcastManager.getInstance(getInstance()).registerReceiver(receiver, filter);  ｝  public static void unregisterLocalReceiver(BroadcastReceiver receiver) {  LocalBroadcastManager.getInstance(getInstance()).unregisterReceiver(receiver);  }  2.如果仅在应用内部通信，可以在AndroidManifest.xml文件中静态注册BroadcastReceiver，同时设置exported="false"。  以下为修复代码示例：  <receiver android:name=".DemoReceiver" android:exported="false" />  3.应用在动态注册BroadcastReceiver时，使用registerReceiver(BroadcastReceiver, IntentFilter, broadcastPermission,android.os.Handle)替代registerReceiver(BroadcastReceiver, IntentFilter)，指定BroadcastReceiver接收时校验permission。 |

### Content Provider数据泄露漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App是否存在Content Provider数据泄露风险。 |
| **危险等级** | 高 |
| **危害** | Content provider可被用于在不同应用程序或者进程之间共享数据，而应用程序的不同数据内容应该具有严格的访问权限。如果权限设置不当，应用程序的content provider数据可能被其他程序直接访问或者修改，导致用户的敏感数据泄露，或者应用数据被恶意篡改，例如盗取账号信息，修改支付金额等。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Activity组件导出风险

|  |  |
| --- | --- |
| **测评目的** | 检测apk中的Activity组件是否存在导出的风险。 |
| **危险等级** | 中 |
| **危害** | Activity作为组成Apk的四个组件之一，是Android程序与用户交互的界面，如果Activity打开了导出权限，可能被系统或者第三方的App直接调出并使用。Activity导出可能导致登录界面被绕过、拒绝服务攻击、程序界面被第三方恶意调用等风险。 |
| **测评结果** | 存在风险(发现1处) |
| **测评结果描述** | 该Apk 中的Activity组件开启了导出权限，存在组件导出风险。 |
| **测评详细信息** | 1.  [文件]：  AndroidManifest.xml  [代码]：  <activity android:name=wintone.idcard.android.IDCardBean android:screenOrientation=0 android:configChanges=0x000000A0> <intent-filter> <action android:name=wintone.idcard> </action> <category android:name=android.intent.category.DEFAULT> </category> </intent-filter> </activity> |
| **解决方案** | 开发者自查：关闭AndroidManifest.xml中的Activity组件导出权限，对于必须导出的组件必须限制于授权用户或者应用组件。 |

### Service组件导出风险

|  |  |
| --- | --- |
| **测评目的** | 检测apk中的Service组件是否存在导出的风险。 |
| **危险等级** | 中 |
| **危害** | Service作为组成Apk的四个组件之一，一般作为后台运行的服务进程，如果设置了导出权限，可能被系统或者第三方的App直接调出并使用。Service导出可能导致拒绝服务攻击，程序功能被第三方恶意调用等风险。 |
| **测评结果** | 存在风险(发现2处) |
| **测评结果描述** | 该Apk 中的Service组件开启了导出权限，存在组件导出风险。 |
| **测评详细信息** | 1.  [文件]：  AndroidManifest.xml  [代码]：  <service android:name=wintone.idcard.android.AuthService android:enabled=true> <intent-filter> <action android:name=wintone.idcard.authService> </action> </intent-filter> </service>  2.  [文件]：  AndroidManifest.xml  [代码]：  <service android:name=wintone.idcard.android.RecogService android:enabled=true> <intent-filter> <action android:name=wintone.idcard.recogService> </action> </intent-filter> </service> |
| **解决方案** | 开发者自查：关闭AndroidManifest.xml中的Service组件导出权限，对于必须导出的组件必须限制于授权用户或者应用组件。 |

### Broadcast Receiver组件导出风险

|  |  |
| --- | --- |
| **测评目的** | 检测apk中的Broadcast Receiver组件是否存在导出的风险。 |
| **危险等级** | 中 |
| **危害** | Broadcast Receiver作为组成Apk的四个组件之一，对外部事件进行过滤接收,并根据消息内容执行响应，如果设置了导出权限，可能被系统或者第三方的App直接调出并使用。Broadcast Receiver导出可能导致敏感信息泄露、登录界面被绕过等风险。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该Apk中的Broadcast Receiver组件无法被导出。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Content Provider组件导出风险

|  |  |
| --- | --- |
| **测评目的** | 检测apk中的Content Provider组件是否存在导出的风险。 |
| **危险等级** | 中 |
| **危害** | Content Provider组成Apk的四个组件之一，是应用程序之间共享数据的容器，可以将应用程序的指定数据集提供给第三方的App，如果设置了导出权限，可能被系统或者第三方的App直接调出并使用。Content Provider导出可能导致程序内部的敏感信息泄露，数据库SQL注入等风险。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该Apk中的Content Provider组件无法被导出。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 本地端口开放越权漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App是否存在本地端口开放的漏洞。 |
| **危险等级** | 中 |
| **危害** | Android应用通常使用PF\_UNIX、PF\_INET、PF\_NETLINK等不同domain的socket来进行本地IPC或者远程网络通信，这些暴露的socket代表了潜在的本地或远程攻击面，特别是PF\_INET类型的网络socket，可以通过网络与Android应用通信，其原本用于linux环境下开放网络服务，由于缺乏对网络调用者身份或者本地调用者id、permission等细粒度的安全检查机制，在实现不当的情况下，可以突破Android的沙箱限制，以被攻击应用的权限执行命令，通常出现比较严重的漏洞，如拒绝服务、root提权或者远程命令执行等。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### PendingIntent错误使用Intent风险

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在PendingIntent使用了隐式Intent或者空Intent的风险。 |
| **危险等级** | 低 |
| **危害** | PendingIntent提供了一种特殊的异步处理机制，App可创建一个待处理的Intent给其他应用，并且允许这个应用以与自己相同的权限来执行这个Intent。即使创建Intent的原始App应用已经被关闭，其他应用在获取PendingIntent之后，仍可能对Intent进行修改，并以原始应用的权限与ID来执行修改后的恶意行为。这样可能导致原始App获取的系统权限和用户数据泄露，例如系统被恶意关闭，短信劫持，系统数据删除，甚至应用中涉及的用户数据被恶意篡改，或者执行恶意操作如转账、发送信息等。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用中不存在PendingIntent错误使用Intent风险。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Intent组件隐式调用风险

|  |  |
| --- | --- |
| **测评目的** | 检测Apk中的Intent组件是否存在隐式调用的风险。 |
| **危险等级** | 低 |
| **危害** | Intent通常用于Activity、Service、Broadcast Receiver等组件之间进行信息传递，包括发送端和接收端。当使用隐式的Intent调用时，并未对intent消息接收端进行限制，因此可能存在该消息被未知的第三方应用劫持的风险。Intent消息被劫持，可能导致用户的敏感数据泄露，或者恶意程序执行等风险。 |
| **测评结果** | 存在风险(发现10处) |
| **测评结果描述** | 该Apk中的intent组件使用了隐式调用的方式，可能存在被劫持的风险。 |
| **测评详细信息** | 1.  [文件]：  com/invs/Blt4$1  [方法]：  public onLeScan(Landroid/bluetooth/BluetoothDevice;I[B)V  2.  [文件]：  com/invs/Blt2  [方法]：  public scanDevice(Z)V  3.  [文件]：  com/invs/BltBase  [方法]：  protected sendMsg(IZ)V  4.  [文件]：  com/invs/Blt2$1  [方法]：  public onReceive(Landroid/content/Context;Landroid/content/Intent;)V  5.  [文件]：  com/invs/BtReaderClient  [方法]：  public sendMsg(Z)V  6.  [文件]：  com/zkc/helper/printer/BlueToothService  [方法]：  public OpenDevice()V  7.  [文件]：  com/yast/yadrly001/MyApplication$1  [方法]：  public handleMessage(Landroid/os/Message;)V  8.  [文件]：  cn/cloudwalk/libproject/Bulider  [方法]：  public setFaceLiveResult(Landroid/content/Context;II)V  9.  [文件]：  cn/cloudwalk/libproject/Bulider  [方法]：  public setFaceResult(Landroid/content/Context;IDLjava/lang/String;Ljava/lang/String;)V  10.  [文件]：  wintone/idcard/android/IDCardBean  [方法]：  public ReturnResultToActivity(Lwintone/idcard/android/ResultMessage;)V |
| **解决方案** | 开发者自查：采用显式方式调用Intent组件，使用指定Intent消息接收方。 |

### Intent Scheme URL攻击漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App应用中是否存在Intent Scheme URL攻击漏洞。 |
| **危险等级** | 中 |
| **危害** | 利用intent scheme URLs(意图协议URL)，可以通过web页面发送intent来启动App应用。攻击者可构造特殊格式的URL直接向系统发送意图，启动App应用的Activity组件或者发送异常数据，导致应用的敏感信息泄露或者应用崩溃。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用不存在Intent Scheme URL攻击漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Fragment注入攻击漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App应用中是否存在Fragment注入攻击漏洞。 |
| **危险等级** | 中 |
| **危害** | Activity可包含多个Fragment来展示界面，PreferenceActivity是支持Fragment的基类activity，其根据传入的参数EXTRA\_SHOW\_FRAGMENT， (‘:android:show\_fragment’)动态创建fragment实现界面展示。 当PreferenceActivity的activity是属性为export，PreferenceActivity不检查传入的参数直接根据其构建对象时，可以构造intent中的extra数据，调用应用内部的任意fragment。fragment注入攻击可导致应用的敏感信息泄露、远程代码执行或者应用崩溃。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用不存在Fragment注入攻击漏洞。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 反射调用风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序是否存在反射调用风险。 |
| **危险等级** | 低 |
| **危害** | 在Java程序中，反射调用可用于强行访问正常途径没有访问权限的代码，在知道目标类的类名和方法名的情况下动态的去调用一些protected甚至是private的方法或类。反射调用在为Java程序对自身进行检查，访问程序的内部属性以及私有方法时提供了便利，但绕过了Java的代码访问权限，也容易留下安全漏洞。使用反射调用机制，可能绕过系统安全设置，访问程序的私有数据，造成用户敏感数据泄露。 |
| **测评结果** | 存在风险(发现10处) |
| **测评结果描述** | 该App存在反射调用风险。 |
| **测评详细信息** | 1.  [文件]：  net/sf/json/JSONObject  [方法]：  private static defaultBeanProcessing(Ljava/lang/Object;Lnet/sf/json/JsonConfig;)Lnet/sf/json/JSONObject;  2.  [文件]：  org/json/JSONObject  [方法]：  public static getNames(Ljava/lang/Object;)[Ljava/lang/String;  3.  [文件]：  org/json/JSONObject  [方法]：  private populateMap(Ljava/lang/Object;)V  4.  [文件]：  com/invs/ClsUtils  [方法]：  public static printAllInform(Ljava/lang/Class;)V  5.  [文件]：  com/ai/smartcrm/activity/CrashHandler  [方法]：  public collectDeviceInfo(Landroid/content/Context;)V  6.  [文件]：  com/sunrise/h/k  [方法]：  public static a(Ljava/lang/Class;Ljava/lang/reflect/Method;)Lcom/sunrise/b/b;  7.  [文件]：  com/sunrise/h/k  [方法]：  public static a(Ljava/lang/Class;Ljava/lang/String;[Ljava/lang/reflect/Field;)Ljava/lang/reflect/Field;  8.  [文件]：  com/sunrise/h/k  [方法]：  public static a(Ljava/lang/Class;Lcom/sunrise/b/d;Ljava/util/Map;Ljava/util/Map;ZLcom/sunrise/a/k;)Ljava/util/List;  9.  [文件]：  com/sunrise/h/h  [方法]：  public static a(Ljava/lang/Class;Ljava/lang/reflect/Type;Lcom/sunrise/a/k;)Lcom/sunrise/h/h;  10.  [文件]：  com/sunrise/d/j  [方法]：  public static a(Ljava/lang/Class;Ljava/util/Map;)V |
| **解决方案** | 开发者自查：  尽量不使用反射调用机制方法，如果一定要用，则对反射所访问的类以及方法进行审计，杜绝隐私数据及关键方法调用。 |

## HTML5安全

### Web Storage数据泄露风险

|  |  |
| --- | --- |
| **测评目的** | 检测App是否存在Web Storage数据泄露风险。 |
| **危险等级** | 低 |
| **危害** | 目前混合开发的App已经越来越多，很多Android App中会使用HTML5开发部分功能，不但可以提供更好的用户体验，也能节省开发资源。这样一来，对于Android App的安全来说，H5的安全也变得不可忽视。 HTML5支持Web Storage，开发者可以为应用创建本地存储，存储一些有用的信息。Web Storage包括LocalStorage和SessionStorage两种，其中LocalStorage可以长期存储，而且存放空间很大，极大的解决了之前只能用Cookie来存储数据的容量小、存取不便、容易被清除的问题。但对与这两种存储方式，攻击者都可以通过XSS攻击窃取信息，获取到存储在其中的敏感信息，如用户名、密码、邮箱等。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App没有使用Web Storage，不存在该风险 |
| **测评详细信息** |  |
| **解决方案** |  |

### WebSQL注入漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App是否存在WebSQL注入漏洞。 |
| **危险等级** | 高 |
| **危害** | 目前很多Android App中会使用HTML5开发部分功能，这样的混合开发方式给厂商带来很多便利，但也需要关注HTML5的安全情况。 HTML5可以在浏览器里面存数据库，如果开发者在开发过程中没有对用户输入的字符串进行过滤，转义，限制或处理不严谨，攻击者就可以通过输入精心构造的字符串去非法获取到数据库中的数据。攻击者通过SQL注入点进行WebSQL攻击，可能导致存储的敏感数据信息被查询泄露，例如账户名，密码等。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App不存在WebSQL注入漏洞 |
| **测评详细信息** |  |
| **解决方案** |  |

### InnerHTML的XSS攻击漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App是否存在InnerHTML的XSS攻击漏洞。 |
| **危险等级** | 高 |
| **危害** | DOM型XSS漏洞是基于文档对象模型（Document Object Model）的一种漏洞。它的攻击代码不需要服务器解析响应，而是通过浏览器端的DOM解析触发XSS。客户端上的JavaScript脚本可以访问浏览器的DOM并修改页面的内容，不依赖服务器的数据，直接从浏览器端获取数据并执行。 在JavaScript中给DOM的innerHTML属性赋值一个<script>标签，是一个非常普遍的xss注入点。如果攻击者利用该漏洞进行攻击，可能会导致账号或Cookie信息被窃取，从而冒充管理者登录后台进行数据篡改等恶意操作。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App不存在InnerHTML的XSS攻击漏洞 |
| **测评详细信息** |  |
| **解决方案** |  |

## 恶意攻击防范能力

### “应用克隆”漏洞攻击风险

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在利用webview跨域访问进行“应用克隆”漏洞攻击的风险。 |
| **危险等级** | 高 |
| **危害** | WebView是Android用于显示网页的控件。当Android应用中存在包含webview的可被导出Activity组件时，若该WebView允许通过file url对http域进行访问，并且未对访问的路径进行严格校验，则可能导致“应用克隆”漏洞攻击。攻击者利用该漏洞，可远程获取用户隐私信息（包括手机应用数据、照片、文档等敏感信息）导致数据泄露，可远程打开并加载恶意HTML文件，甚至获取App中包括用户登录凭证在内的所有本地敏感数据。 |
| **测评结果** | 存在风险(发现1处) |
| **测评结果描述** | 该App程序存在利用“应用克隆”漏洞进行攻击的风险。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private initWebView()V |
| **解决方案** | 开发者自查：  1.严格限制包含WebView调用的Activity组件的导出权限，关闭导出权限或者限制导出组件的发起者。  2.对于功能要求必须导出的Activity组件，手动设置  setAllowFileAccessFromFileURLs（false）或  setAllowUniversalAccessFromFileURLs（false）  或者设置minSDK不小于16,因为此时这两处API默认为false  3. 对于必须使用file URL对http域进行访问时，可对传入的URL路径范围严格控制，例如建立URL白名单，设置允许访问的URL列表（不要遗漏路径中可能出现的特殊情况如“../../”等，避免限制被绕过）。示例代码如下 ：  /\*构建webview\*/  WebView webView = new WebView(this);  webview.setWebViewClient(new WebViewClient{  public boolean shouldOverrideUrlLoading(WebView view, String url){  /\*白名单\*/  String[] allowUrlArr = {  "a.html",  "b.html",  "c.js",  }  /\*禁止url中出现../避免白名单被绕过\*/  if(-1 != url.indexOf("../")){  return true;  }  /\*应用自己的HTML文件放在/data/data/(app)目录下，避免被第三方替换或修改\*/  if(url.startsWith("/data/data/(app)")){  /\*检测重定向的url是否在白名单中\*/  for(String s : allowUrlArr){  if(url.endsWith(s)){  return false;  }  }  }  return true;  }  })  当返回值为true时，应该拒绝此URL路径下的访问。 |

### 动态注入攻击风险

|  |  |
| --- | --- |
| **测评目的** | 检测客户端App运行时是否面临动态注入的风险。 |
| **危险等级** | 高 |
| **危害** | 动态注入是指通过OS特定机制，利用系统API将代码写入到目标进程并让其执行。通过动态注入，攻击者可以将一段恶意代码写到目标进程，这段代码可以加载其它可执行程序，进而实施hook，监控程序运行、获取敏感信息等。常见的动态注入，可以实现窃取输入的登录账号、密码、支付密码，修改转账的目标账号、金额，窃取通讯数据等。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Webview远程代码执行漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测app应用的webview组件中是否存在远程代码执行漏洞。 |
| **危险等级** | 高 |
| **危害** | Webview是Android用于浏览网页的组件，其包含的接口函数addJavascriptInterface可以将Java类或方法导出以供JavaScript调用，实现网页JS与本地JAVA的交互。由于系统没有限制已注册JAVA类的方法调用，因此未注册的其它任何JAVA类也可以被反射机制调用，这样可能导致被篡改的URL中存在的恶意代码被执行，用户手机被安装木马程序，发送扣费短信，通信录或者短信被窃取，甚至手机被远程控制。 |
| **测评结果** | 存在漏洞(发现1处) |
| **测评结果描述** | 该App应用中可能存在被addJavascriptInterface接口导出的未注册Java类函数。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/activity/MainActivity |
| **解决方案** | 开发者自查：取消使用addJavascriptInterface接口，以其他Java与JavaScript互通方案代替；若必须使用，则应对访问的url进行过滤限制或对html页面进行完整性校验，同时显示移除对指定的javascript接口的调用： removeJavascriptInterface ("searchBoxJavaBridge\_"); removeJavascriptInterface ("accessibility"); removeJavascriptInterface ("accessibilityTraversal")；。 |

### 未移除有风险的Webview系统隐藏接口漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App程序中是否已经移除有风险的Webview系统隐藏接口。 |
| **危险等级** | 高 |
| **危害** | Webview远程代码执行最早在CVE-2012-663中被发现，起初产生的原因是由于WebView addJavascriptInterface接口引起的。在2014年公布的CVE-2014-1939中，研究人员发现在Android系统中android/webkit/webview中默认内置的一个searchBoxJavaBridge\_ API 同时存在远程代码执行漏洞。而最近公布的一次关于WebView远程代码执行的漏洞是CVE-2014-7224，其中发现的是两个新的攻击向量存在于android/webkit/AccessibilityInjector.java中,这两个接口分别是”accessibility” 和”accessibilityTraversal”，调用了此组件的应用在开启了辅助功能选项中第三方服务的安卓系统上也将面临远程代码执行漏洞。 |
| **测评结果** | 存在漏洞(发现1处) |
| **测评结果描述** | 该App程序中未移除有风险的Webview系统隐藏接口。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/activity/MainActivity |
| **解决方案** | 开发者自查：开发者显式移除有风险的Webview系统隐藏接口。  以下为修复代码示例：  在使用Webview加载页面之前，执行  webView.removeJavascriptInterface("searchBoxJavaBridge\_");  webView.removeJavascriptInterface("accessibility");  webView.removeJavascriptInterface("accessibilityTraversal"); |

### zip文件解压目录遍历漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在解压zip文件时可导致目录遍历的漏洞 |
| **危险等级** | 中 |
| **危害** | App在运行过程中，可能对下载的或者本地存储中的zip格式文件进行解压。由于在zip压缩包下的文件路径名中允许存在“../”字符串，而“../”在Android系统中将被解释为返回上层目录，那么攻击者可能利用多个“../”构造出不安全的zip压缩包。当app程序中使用ZipEntry.getName()解压zip文件时，没有对上级目录字符串(../)进行过滤校验，可能会导致被解压的文件发生目录跳转，解压到当前目录以外的其他目录，并且覆盖应用原有的文件。如果被覆盖掉的文件是js、so和dex等文件，可能导致拒绝服务攻击，甚至是恶意代码执行。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App中不存在解压zip文件导致目录遍历的漏洞 |
| **测评详细信息** |  |
| **解决方案** |  |

### 下载任意apk漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测应用中是否存在下载任意apk的漏洞。 |
| **危险等级** | 高 |
| **危害** | 具有下载apk功能的组件存在导出漏洞，并且未对组件调用者进行校验。攻击者可利用导出组件的手段下载攻击者指定的任意apk文件，并且在下载过程中伪装apk文件的下载信息，例如图标、描述等，导致用户被诱导下载安装恶意应用。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App应用中不存在可被导出的具有下载apk功能的组件。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 拒绝服务攻击漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App应用中的组件是否存在拒绝服务攻击的漏洞。 |
| **危险等级** | 中 |
| **危害** | Intent通常用于Activity、Service、Broadcast Receiver等组件之间进行信息传递，其负责对应用中一次操作的动作及数据进行描述。当intent中包含空数据、异常或者畸形数据时，如果Android应用程序没有对Intent.getXXXExtra()获取的异常或者畸形数据进行异常捕获，那么可导致接收该Intent的应用崩溃。拒绝服务攻击漏洞可能导致安全防护、监控类应用失效，也可能导致应用被大面积恶意攻击而崩溃，造成经济利益损失或者客户流失。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 从sdcard加载dex风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序中的是否存在从sdcard动态加载dex的风险。 |
| **危险等级** | 中 |
| **危害** | 低于Anroid4.1的系统版本允许APP动态加载存储在sdcard的dex文件，该目录也可被其他应用读写。当APP对于从外部加载的DEX文件未做完整性校验时，向加载的dex注入恶意代码或者使用恶意代码替换dex文件，将会导致恶意代码执行。常见的恶意代码，可能导致登录账号、密码、支付密码被窃取，恶意扣费，病毒注入等风险。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App程序中不存在从sdcard加载dex文件的行为。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 从sdcard加载so风险

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在从sdcard动态加载so的风险。 |
| **危险等级** | 中 |
| **危害** | 出于节省Apk包大小，或者动态升级so文件的原因，App程序可能将部分so文件存储或者下载于sdcard上，然后进行动态加载。为成功动态加载so文件，App首先将so文件读取到应用私有目录下，再使用system.load函数加载该目录下的so文件，并且该目录是应用私有目录（/data/data/<packagename>/）下的非默认lib库文件夹。该过程中APP动态加载了存储在sdcard上的so文件，如果存储的so文件被存在恶意行为的so文件替换，将会导致恶意代码执行。常见的恶意代码，可能导致登录账号、密码、支付密码被窃取，恶意扣费，病毒注入等风险。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App中不存在从sdcard加载so文件的行为。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 未使用编译器堆栈保护技术风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序中是否存在未使用编译器堆栈保护技术风险。 |
| **危险等级** | 低 |
| **危害** | 缓冲区溢出攻击是指当程序向内存缓冲区内填充数据位数时超过了缓冲区本身的容量，导致溢出的数据覆盖在合法数据上，从而修改内存中将执行的程序地址。这种攻击通常发生在堆栈中，攻击者需要事先分析被攻击进程的虚拟地址空间布局，然后采用硬编码方式向堆栈缓冲区填充恶意代码。如果系统每次加载应用进程和动态链接库时，基地址都加载到固定虚拟内存地址处，攻击者可得出应用程序的地址空间布局，便可以通过构造恶意的缓冲区数据，使该函数返回时跳转至攻击者注入的恶意代码或 shellcode 处执行。缓冲区溢出攻击，可能导致程序执行失败、系统宕机或者恶意程序执行等后果，造成用户数据泄露或者对手机系统实现恶意操作。攻击者利用堆栈溢出漏洞时，通常会破坏当前的函数栈。Stack Canaries漏洞探测技术，可以对缓冲区溢出进行预警。在所有函数调用发生时，向栈帧内压入一个被称作canary的随机数，当栈中发生溢出时，canary将被首先覆盖，之后才是EBP和返回地址。在函数返回之前，系统通过检测栈帧中的canary数值是否发生变化来判断是否发生了栈溢出漏洞，此时程序将跳转到stack\_chk\_fail输出错误消息并终止执行。 |
| **测评结果** | 存在风险(发现4处) |
| **测评结果描述** | 该App程序中未使用编译器堆栈保护技术。 |
| **测评详细信息** | 1.  [文件]：  lib/mips64/libinvswlt.so  2.  [文件]：  lib/mips/libinvswlt.so  3.  [文件]：  lib/armeabi/libDecodeWlt.so  4.  [文件]：  lib/armeabi/libopencv\_java.so |
| **解决方案** | 开发者自查：开发者应该在编译Native程序即so文件时使用Canary探测技术，防止缓冲区溢出攻击的发生。  以下为修复代码示例:  在生成so文件库时，使用以下参数：  gcc -o DemoCanary DemoCanary.c -fstack-protector-all |

### 未使用地址空间随机化技术风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序中是否存在未使用地址空间随机化技术风险。 |
| **危险等级** | 低 |
| **危害** | 应用程序的地址空间布局是固定的，自低向高依次为代码区，BSS区，堆栈区，攻击者通过分析能轻易得出各区域的基地址。基于这些信息，只要攻击者的注入代码被执行，攻击程序就能随意跳转到其指定的内存区域，最终获取系统的控制权。而地址空间随机化技术的基本思想，则是动态随机分配内存地址给程序代码区，BSS区，堆栈区的基地址，即使攻击者注入的代码被执行，也会因为无法找到合法的返回地址而产生错误，最终攻击进程无法执行。ASLR（Address space layout randomization）是一种针对缓冲区溢出的安全保护技术。 |
| **测评结果** | 安全 |
| **测评结果描述** | 该App程序中已经使用了使用地址空间随机化技术。 |
| **测评详细信息** |  |
| **解决方案** |  |

### Root设备运行风险

|  |  |
| --- | --- |
| **测评目的** | 检测App程序是否可以在被Root的手机设备中运行。 |
| **危险等级** | 低 |
| **危害** | 为了获取更大的手机自主使用功能，如卸载应用、禁用自启动程序等，不少用户会将手机进行Root处理以获取Root权限。Root权限包括：超越任何用户和用户组来对文件或目录进行读取、修改或删除；对可执行程序的执行、终止；对硬件设备的添加、创建和移除等；也可以对文件和目录进行属主和权限进行修改，以适合系统管理的需要。获取Android的Root权限通常是通过系统漏洞，替换或添加可绕过用户验证的可执行SU程序。在给手机用户赋予Root权限的同时，也给了其他应用获取Root权限的可能性。恶意程序可能在用户不知情的情况下申请Root权限，读取到其他应用的文件或者进程中的敏感信息，例如支付宝、手机银行等应用的账号和密码等；或者任意读取手机中的短信记录和联系人信息；也可能获取到系统权限的重启功能，恶意重启或关闭设备。 |
| **测评结果** | 未执行 |
| **测评结果描述** | 该应用在该项测评过程中出现异常，可能由于未知原因导致该项自动测评执行失效。该应用无法执行该测评项目。 |
| **测评详细信息** |  |
| **解决方案** |  |

### 不安全的浏览器调用漏洞

|  |  |
| --- | --- |
| **测评目的** | 检测App中是否存在不安全的浏览器调用漏洞。 |
| **危险等级** | 中 |
| **危害** | Chrome V8引擎3.20至4.2版本中存在远程代码执行漏洞（CNNVD-201608-414）。该漏洞是由于源代码中“observe\_accept\_invalid”异常类型被误写为“observe\_invalid\_accept”，造成kMessages关键对象信息泄露，从而可利用该漏洞执行任意代码。远程攻击者可通过诱使用户扫描二维码或者诱使用户点击恶意链接对应用进行攻击，可能导致用户隐私泄露，如通讯录，短信，录音，录像等；用户财产损失，如窃取支付密码、钱包密码等；远程控制手机等。 |
| **测评结果** | 存在漏洞(发现1处) |
| **测评结果描述** | 该App中存在不安全的浏览器调用漏洞。 |
| **测评详细信息** | 1.  [文件]：  com/ai/smartcrm/activity/MainActivity  [方法]：  private initWebView()V |
| **解决方案** | 开发者自查：  1.开发者需要在应用调用外部浏览器时对引擎版本进行检测，当发现调用Chrome V8引擎并且版本低于4.2时停止调用外部浏览器并且提示用户对调用的系统浏览器进行升级或者修改系统默认的浏览器。  2.集成第三方sdk实现浏览器功能，如腾讯的x5sdk(最新版)。 |

# App安全测评依据

《信息安全技术 公共及商用服务信息系统个人信息保护指南》《信息安全技术 移动智能终端个人信息保护技术要求》《YD/T 1438-2006 数字移动台应用层软件功能要求和测试方法》《YD/T 2307-2011 数字移动通信终端通用功能技术要求和测试方法》《电子银行业务管理办法》《电子银行安全评估指引》《中国金融移动支付客户端技术规范》《中国金融移动支付应用安全规范》

# 附录A：安全漏洞危险等级评定标准

该平台在移动应用的安全漏洞危险等级划分上，参考了中华人民共和国国家标准《信息安全技术-安全漏洞等级划分指南》（GB/T 30279-2013），该标准是由中国信息安全测评中心、中国科学院研究生院国家计算机网络入侵防范中心和北京航空航天大学起草，由国家质量监督检验检疫总局和多家标准化管理委员会联合发布。

国标《信息安全技术-安全漏洞等级划分指南》（GB/T 30279-2013）从安全漏洞的访问路径、利用复杂度和影响程度三个方面对安全漏洞进行评估，准确与合理的划分出安全漏洞的危险等级。

1. 访问路径

访问路径：攻击者利用安全漏洞影响目标系统的路径前提。

|  |  |
| --- | --- |
| 访问路径 | 描述 |
| 本地 | 利用该安全漏洞要求攻击者物理接触到受攻击的系统，或者已具有一个本地账号 |
| 邻接 | 利用该安全漏洞要求攻击者与受攻击系统同处于一个广播域或冲突域中 |
| 远程 | 不局限于本地和邻接 |

1. 利用复杂度

利用复杂度：对于安全漏洞可被利用于影响目标系统的技术、环境等条件的难度。

|  |  |
| --- | --- |
| 攻击复杂度 | 描述 |
| 简单 | 无需借助外部条件 |
| 复杂 | 需要借助外部条件 |

1. 影响程度

影响程度：利用安全漏洞对目标系统造成的损害程度。

|  |  |
| --- | --- |
| 考量维度 | 描述 |
| 完整性 | 保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性 |
| 可用性 | 数据或资源的特性，被授权实体按要求能访问和使用数据或资源 |
| 保密性 | 数据所具有的特性，即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度 |

影响程度依据完整性、可用性、保密性的影响进行赋值，影响程度从高到低包括完全、部分、轻微和无。

1. 风险等级评估表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **利用复杂度** | **影响程度** | **访问路径及安全漏洞等级** | | |
| 远程 | 邻接 | 本地 |
| 简单 | 完全 | 高 | 高 | 高 |
| 部分 | 高 | 中 | 中 |
| 轻微 | 中 | 低 | 低 |
| 复杂 | 完全 | 高 | 高 | 中 |
| 部分 | 中 | 低 | 低 |
| 轻微 | 低 | 低 | 低 |