

SoftSec

9dd8ecd72a1e525f03fb1796c69103a8缺陷分析报告

2017-04-07 08:36:18



检测报告

1. 应用程序基本信息

应用名称： '动游游戏大厅'

版本信息： 2. 2. 0718. 1

系统平台： 支持android 2.2及以上版本

MD5值： 9dd8ecd72a1e525f03fb1796c69103a8

检测时间： 2017-04-07 08:35:53

结束时间： 2017-04-07 08:36:18

检测人员： SOFTSEC

2. 检测说明

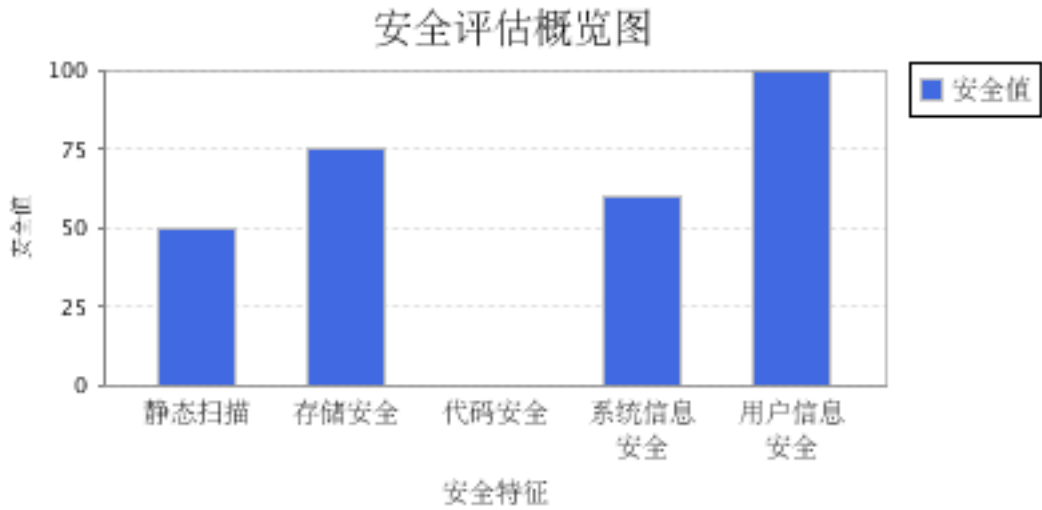
检测环境： 自动化静态检测实验室

检测方法： 使用静态检测方法，配合静态扫描和规则库，发现应用程序可能存在的缺陷，并提出相关建议。

3. 检测结果概览

柱状图中包含静态安全、存储安全、代码安全、系统信息安全、用户信息安全共5项。

柱状图中,安全项若有蓝色柱体越高则表示该安全项越安全，若无蓝色柱体则表示未采取安全措施。



4. 检测结果详情

4.1. 静态扫描结果详情

(1) 文件扫描
对安装包的内部文件扫描,发现特殊文件和敏感信息，特殊文件列表如下：
libdybadminton20.so
libdybasketball.so
libdybowling.so

libdyfifo. so
libdyjetski20. so
libdybow20. so
libdygameinterface. so
libdykingogboxing20. so
libdyrushhours20. so

(2) APP反编译

此应用程序不能进行反编译。

(3) APP篡改

此应用程序不能进行篡改。

描述：此应用程序经过apktool检测到完整性校验步骤，表明此应用程序有完整性校验服务，无法重新打包为完整的应用程序，所以无法进行反编译和篡改。

危害：无。

建议：无。

(4) 权限设计

扫描安装包权限,发现使用较多权限，使用的权限列表如下：

android.permission.READ_PHONE_STATE
android.permission.INJECT_EVENT
android.permission.SYSTEM_ALERT_WINDOW
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.BLUETOOTH
android.permission.INTERNET
android.permission.CHANGE_WIFI_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.BLUETOOTH_ADMIN
android.permission.WAKE_LOCK
android.permission.ACCESS_NETWORK_STATE
android.permission.KILL_BACKGROUND_PROCESSES

4.2. 存储安全结果详情

(1) 存储权限

扫描存储权限,该应用程序可能会使用SD卡。

(2) 通讯录

该应用程序没有对通讯录进行读写。

(3) 通话记录

该应用没有对通话记录进行读写。

(4) 短信记录

该应用程序没有对短信记录进行读写。

4.3. 代码安全结果详情

(1) 源代码混淆

此应用程序未混淆。

描述：此应用程序中含有R和其子类，表明未曾优化和混淆。
危害：未混淆的应用程序反编译后的代码容易阅读，极易容易被篡改和被盗。
建议：进行混淆处理。

(2) 明文字符串

此应用程序资源使用信息未经过处理。

描述：此应用程序中含有明文存储的URL、电话号码等敏感信息。

危害：没有隐藏程序资源使用信息，资源使用信息容易泄露，被攻击者盗用、篡改，生成钓鱼App，导致您App名誉受损，收益减少。

建议：对资源使用信息进行隐藏处理。

此应用程序中含有明文存储的URL、电话号码等敏感信息，这些信息如下所示。

http://download.aiwi-game.com.cn/dygame/android/
http://download.aiwi-game.com.cn/dygame/android/game_zone_pic.zip
http://api.dygame.cn/api/api/clientReg?
http://baoku.360.cn/soft/show/appid/103150776
http://books.google.
http://baoku.360.cn/soft/show/appid/103150789
http://google.com/books
http://www.dygame.cn/download_qr.html?DYGAME:
http://static.apc.360.cn/cms/game/dongyou.html
http://www.google
http://code.google.com/p/zxing/wiki/FrequentlyAskedQuestions
http://interface.appstore.huan.tv/service/appstore/game/getAppInfosByDevname
http://download.aiwi-game.com.cn/dygame/game_zone/
http://api.dygame.cn/api/api/clientLogin?
http://www.dygame.cn
https://www.google.com.tw/
http://api.dygame.cn/user360/yacht#
http://code.google.com/p/zxing
http://www.dygame.cn/download_qr.html
http://
http://zxing.appspot.com/scan
192.168.43.30

4.4. 系统信息安全结果详情

(1) IMSI/IMEI

该应用程序未读取用户码/设备码。

(2) 操作系统版本

该应用程序未读取系统型号、版本、配置信息。

(3) GPS信息

该应用程序未读取地理位置信息。

(4) 蓝牙信息

该应用程序能够读取蓝牙开启检测信息，详细信息如下：

文件名	Lcom/dygame/gamezone2/QRCodeContent;
风险等级	3
行号	3814
方法名	getDefaultAdapter
规则ID	1-2-2-1
规则类别	自动开启蓝牙
详细描述	自动开启蓝牙.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称: GetQRCodeContent 调用语句: invoke-static []Landroid/bluetooth/BluetoothAdapter; getDefaultAdapter Landroid/bluetooth/BluetoothAdapter;

文件名	Lcom/dygame/gamezone2/Logo;
风险等级	3
行号	1486
方法名	getDefaultAdapter
规则ID	1-2-2-1
规则类别	自动开启蓝牙
详细描述	自动开启蓝牙.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称: setupHotspotBluetooth 调用语句: invoke-static []Landroid/bluetooth/BluetoothAdapter; getDefaultAdapter Landroid/bluetooth/BluetoothAdapter;

文件名	Lcom/dygame/gamezone2/BluetoothServer\$AcceptThread;
风险等级	3
行号	67
方法名	getDefaultAdapter
规则ID	1-2-2-1
规则类别	自动开启蓝牙
详细描述	自动开启蓝牙.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称: <init> 调用语句: invoke-static []Landroid/bluetooth/BluetoothAdapter; getDefaultAdapter Landroid/bluetooth/BluetoothAdapter;

文件名	Lcom/dygame/gamezone2/BluetoothServer;
风险等级	3
行号	90
方法名	getDefaultAdapter
规则ID	1-2-2-1
规则类别	自动开启蓝牙
详细描述	自动开启蓝牙.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称: <init> 调用语句: invoke-static []Landroid/bluetooth/BluetoothAdapter; getDefaultAdapter Landroid/bluetooth/BluetoothAdapter;

(5) wifi信息

该应用程序能够读取WiFi信息，详细信息如下：

文件名	Lcom/dygame/gamezone2/wifi/AlWifiManager;
风险等级	2
行号	221
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:connect 调用语句:invoke-virtual [v4]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/wifi/AlWifiManager;
风险等级	2
行号	188
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:connect 调用语句:invoke-virtual [v4]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/wifi/AlWifiManager;
风险等级	2
行号	441
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:findNetworkInExistingConfig 调用语句:invoke-virtual [p1]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/wifi/AlWifiManager;
风险等级	2
行号	1280
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:enableAllNetwork 调用语句:invoke-virtual [v2]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/wifi/AlWifiManager;
风险等级	3
行号	1442
方法名	setWifiEnabled

规则ID	1-2-1-1
规则类别	自动开启wifi
详细描述	自动开启wifi.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:setWifiEnabled 调用语句:invoke-virtual [v3, p1]Landroid/net/wifi/WifiManager; setWifiEnabled Z Z

文件名	Lcom/dygame/gamezone2/ConnectMobileHotspot\$2;
风险等级	3
行号	171
方法名	setWifiEnabled
规则ID	1-2-1-1
规则类别	自动开启wifi
详细描述	自动开启wifi.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:run 调用语句:invoke-virtual [v2, v9, v3, v4]Lcom/dygame/gamezone2/wifi/AlWifiManager; setWifiEnabled Z ZJ

文件名	Lcom/dygame/gamezone2/HotSpot;
风险等级	1
行号	1387
方法名	getConnectionInfo
规则ID	1-2-1-3
规则类别	得到wifi配置信息
详细描述	得到wifi配置信息.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:setWifiApEnabled 调用语句:invoke-virtual/range [v17, v17]Landroid/net/wifi/WifiManager; getConnectionInfo Landroid/net/wifi/WifiInfo;

文件名	Lcom/dygame/gamezone2/HotSpot;
风险等级	3
行号	1402
方法名	setWifiEnabled
规则ID	1-2-1-1
规则类别	自动开启wifi
详细描述	自动开启wifi.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:setWifiApEnabled 调用语句:invoke-virtual/range [v17, v18]Landroid/net/wifi/WifiManager; setWifiEnabled Z Z

文件名	Lcom/dygame/gamezone2/HotSpot;
风险等级	3
行号	2061
方法名	setWifiEnabled
规则ID	1-2-1-1
规则类别	自动开启wifi
详细描述	自动开启wifi.

时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:setWifiApEnabled 调用语句:invoke-virtual/range [v17, v18]Landroid/net/wifi/WifiManager; setWifiEnabled Z Z

文件名	Lcom/dygame/gamezone2/HotSpot;
风险等级	3
行号	1428
方法名	setWifiEnabled
规则ID	1-2-1-1
规则类别	自动开启wifi
详细描述	自动开启wifi.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:setWifiApEnabled 调用语句:invoke-virtual/range [v17, v18]Landroid/net/wifi/WifiManager; setWifiEnabled Z Z

文件名	Lcom/dygame/gamezone2/wifi/ReenableAllApsWhenNetworkStateChanged;
风险等级	2
行号	51
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:reenableAllAps 调用语句:invoke-virtual [v2]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/QRCodeContent;
风险等级	1
行号	3669
方法名	getConnectionInfo
规则ID	1-2-1-3
规则类别	得到wifi配置信息
详细描述	得到wifi配置信息.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:GetQRCodeContent 调用语句:invoke-virtual [v9]Landroid/net/wifi/WifiManager; getConnectionInfo Landroid/net/wifi/WifiInfo;

文件名	Lcom/dygame/gamezone2/QRCodeContent;
风险等级	2
行号	3705
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:GetQRCodeContent 调用语句:invoke-virtual [v9]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/wifi/Wifi;
风险等级	2
行号	99
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:checkForExcessOpenNetworkAndSave 调用语句:invoke-virtual [p0]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/wifi/Wifi;
风险等级	2
行号	556
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:getMaxPriority 调用语句:invoke-virtual [p0]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/wifi/Wifi;
风险等级	2
行号	657
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:getWifiConfiguration 调用语句:invoke-virtual [p0]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/wifi/Wifi;
风险等级	2
行号	785
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:getWifiConfiguration 调用语句:invoke-virtual [p0]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/wifi/Wifi;
风险等级	2

行号	869
方法名	getConfiguredNetworks
规则ID	1-2-1-2
规则类别	得到wifi网络信息
详细描述	得到wifi网络信息
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:shiftPriorityAndSave 调用语句:invoke-virtual [p0]Landroid/net/wifi/WifiManager; getConfiguredNetworks Ljava/util/List;

文件名	Lcom/dygame/gamezone2/Utility;
风险等级	1
行号	1200
方法名	getConnectionInfo
规则ID	1-2-1-3
规则类别	得到wifi配置信息
详细描述	得到wifi配置信息.
时间	2017年04月07日08时36分06秒
具体敏感调用信息	函数名称:GetLocalMacAddress 调用语句:invoke-virtual [v2]Landroid/net/wifi/WifiManager; getConnectionInfo Landroid/net/wifi/WifiInfo;

4.5. 用户信息安全结果详情

(1) 用户电话号码信息

该应用程序未读取用户电话号码信息。