Static Analysis - com.fdhgkjhrtjkjbx.model.apk

APP SCORE

Average CVSS Score: 7.5

App Security Score: 85/100

Trackers Detection: 0/227

FILE INFORMATION

Name: com.fdhgkjhrtjkjbx.model.apk

Size: 2.4MB

MD5: 3d7e04e37db833f47d08975e27c69a9c

SHA1: 91a302f1a2cac8951123431f75ff8d705950fb17

SHA256: 9a0dfff4d05e739d53da02e9275b67dcff6ca1fdd82d65cb2c06b96b90fa3

APP INFORMATION

Name: □□□□□□□

Package Name: com.fdhgkjhrtjkjbx.model

Main Activity: .LoadActivity

Target SDK: 19

Min SDK: 10

Max SDK:

Android Version Name: 5.0

Android Version Code: 5

PLAY STORE INFORMATION

CERTIFICATE

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=rt, ST=tcvjdb, L=sfgjfdghf, O=rtghmxcj, OU=sfzdhjhk, CN=h
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-08-26 04:36:12+00:00
Valid To: 2069-05-29 04:36:12+00:00
Issuer: C=rt, ST=tcvjdb, L=sfgjfdghf, O=rtghmxcj, OU=sfzdhjhk, CN=hg
Serial Number: 0x53fc0ebc
Hash Algorithm: sha1
md5: 248961c8d91835a69805365555cfb30c
sha1: f89216d7dfc56433d0d77590ef89edaaa50dc07b
sha256: 869b0f220e69963e9c94aa810a570eebb058693f716172262c1
sha512: 5e3af9525fa6f5c3217e737e28ef5a98fc0e58c37074781b5560d

Certificate Status: Bad
Description: The app is signed with `SHA1withRSA`. SHA1 hash algorit

PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
com.android.launcher.permission.INSTALL_SHORTCUT	normal		Allows an application to install a shortcut in Launcher.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.

ANDROID LIBRARY BINARY ANALYSIS

ISSUE	SEVERITY	DESCRIPTION	FILES
Found elf built without Position Independent Executable (PIE) flag	high	In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries. Built with option -pie.	lib/armeabi/libsecmain.so lib/armeabi/libsecexe.so

APKiD ANALYSIS

APKiD not enabled.

FILE

BROWSABLE ACTIVITIES

ACTIVITY INTENT

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Application Data can be Backed up [android:allowBackup=true]	medium	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
Broadcast Receiver (com.yangccaa.chengaa.WEPP) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Launch Mode of Activity (com.yangccaa.ssll.SDGG) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
Broadcast Receiver (com.yangccaa.ssll.SDHH) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

CODE ANALYSIS

ISSUE	SEVERITY	CVSS	CWE	OWASP	FILES
MD5 is a weak hash known to have hash collisions.	high	**7.4**	**CWE-327**	**M5: Insufficient Cryptography**	com/bangcle/protect/Util.java
The App logs information. Sensitive information should never be logged.	info	**7.5**	**CWE-532**		com/bangcle/protect/Util.java

ANDROID API

API	FILES
Dynamic Class and Dexloading	com/fdhgkjhrtjkjbx/model/BaseApp.java com/bangcle/protect/MyClassLoader.java
Java Reflection	com/fdhgkjhrtjkjbx/model/BaseApp.java com/bangcle/protect/Util.java
Loading Native Code (Shared Library)	com/bangcle/protect/ACall.java
Content Provider	com/bangcle/protect/ACall.java com/bangcle/protect/Util.java
Execute OS Command	com/bangcle/protect/Util.java
Message Digest	com/bangcle/protect/Util.java
Inter Process Communication	com/yangccaa/ssll/SDHH.java com/yangccaa/chengaa/WEPP.java

URLS

FIREBASE DATABASES

MALWARE CHECK

EMAILS

TRACKERS

Tracker Name	URL

FILE ANALYSIS

ISSUE	FILES
Certificate/Key Files Hardcoded inside the App.	assets/meta-data/rsa.pub

STRINGS

"app_name" : "□□□□□□□"
"action_settings" : "Settings"
"main1" : "□□"
"main2" : "□□"
"main3" : "□□"
"main4" : "□□"
"main5" : "□□"
"newMiddleText1" : "□□□□"
"newMiddleText2" : "□□□□"
"newMiddleText3" : "□□□□"
"newMiddleText4" : "□□□□"
"newText1" : "□□1"
"searchbut1" : "□□"
"searchbut2" : "□□"
"searchbut3" : "□□"
"searchbut4" : "□□"
"searchbut5" : "□□"
"searchbut6" : "□□"
"searchbut7" : "□□□"

ACTIVITIES

.LoadActivity
.BgActivity
.MainActivity
.NewActivity
.ReadActivity
.DingActivity
.SearchActivity
.ShowSearchActivity
.SitemActivity
.MoreActivity
.ShowHtmlActivity
.ShowActivity
.AppStoreActivity
.AppDetailActivity
.MakeMoneyActivity
.ExchangeActivity
com.jfdlplapk.BiwlzuGoogleActivity
com.yangccaa.chengaa.WEYY
com.yangccaa.ssll.SDGG

PROVIDERS

RECEIVERS

com.yangccaa.chengaa.WEPP
com.yangccaa.ssll.SDHH

SERVICES

.MainService
.FloatService
.CloseAdvService
com.jfdlplapk.BiwlzuGoogleService
com.yangccaa.chengaa.WEUU
com.yangccaa.ssll.SDKK

LIBRARIES

FILES

META-INF/MANIFEST.MF
META-INF/HJGHGVZ_.SF
META-INF/HJGHGVZ_.RSA
assets/meta-data/manifest.mf
assets/meta-data/rsa.pub
assets/meta-data/rsa.sig
AndroidManifest.xml
assets/WWF0
assets/adv.xml
assets/bangcle_classes.jar
assets/com.fdhgkjhrtjkjbx.model
assets/com.fdhgkjhrtjkjbx.model.art
assets/com.fdhgkjhrtjkjbx.model.x86
assets/ding1.html

assets/ding10.html
assets/ding2.html
assets/ding3.html
assets/ding4.html
assets/ding5.html
assets/ding6.html
assets/ding7.html
assets/ding8.html
assets/ding9.html
assets/dinglist.xml
assets/dyjn
assets/libsecexe.x86.so
assets/libsecmain.x86.so
assets/new.xml
assets/read1.html
assets/read2.html
assets/read3.html
assets/read4.html
assets/read5.html
assets/read6.html
assets/read7.html
assets/read8.html
assets/read9.html
assets/readlist.xml
assets/search.xml
classes.dex
lib/armeabi/libsecexe.so
lib/armeabi/libsecmain.so
res/drawable-hdpi/advance.png
res/drawable-hdpi/back.png
res/drawable-hdpi/bg.jpg
res/drawable-hdpi/bg_listview_item_normal.png
res/drawable-hdpi/bg_listview_item_pressed.png
res/drawable-hdpi/biao.png
res/drawable-hdpi/btn_back.png
res/drawable-hdpi/btn_submit.png
res/drawable-hdpi/btn_submit_press.png
res/drawable-hdpi/button_back.png
res/drawable-hdpi/button_download_normal.png
res/drawable-hdpi/button_download_pressed.png
res/drawable-hdpi/button_price_normal.png
res/drawable-hdpi/button_price_pressed.png
res/drawable-hdpi/button_title_back_normal.png
res/drawable-hdpi/button_title_back_pressed.png

res/drawable-hdpi/clear.png
res/drawable-hdpi/content_edit.png
res/drawable-hdpi/daily_update_bg.png
res/drawable-hdpi/dui_focus.png
res/drawable-hdpi/dui_normal.png
res/drawable-hdpi/feature_point.png
res/drawable-hdpi/feature_point_cur.png
res/drawable-hdpi/game_halfstar.png
res/drawable-hdpi/game_star.png
res/drawable-hdpi/head.png
res/drawable-hdpi/home_btn_bg_d.png
res/drawable-hdpi/home_btn_bg_n.png
res/drawable-hdpi/home_btn_bg_s.png
res/drawable-hdpi/huafei.png
res/drawable-hdpi/ic_launcher.png
res/drawable-hdpi/icon.png
res/drawable-hdpi/icon_1_n.png
res/drawable-hdpi/icon_1_ns.png
res/drawable-hdpi/icon_2_n.png
res/drawable-hdpi/icon_2_ns.png
res/drawable-hdpi/icon_3_n.png
res/drawable-hdpi/icon_3_ns.png
res/drawable-hdpi/icon_4_n.png
res/drawable-hdpi/icon_4_ns.png
res/drawable-hdpi/icon_5_n.png
res/drawable-hdpi/icon_5_ns.png
res/drawable-hdpi/image_app_introduce_normal.png
res/drawable-hdpi/image_app_introduce_pressed.png
res/drawable-hdpi/image_app_reference_normal.png
res/drawable-hdpi/image_app_reference_pressed.png
res/drawable-hdpi/img_coin.png
res/drawable-hdpi/line.png
res/drawable-hdpi/load.gif
res/drawable-hdpi/maintab_toolbar_bg.png
res/drawable-hdpi/make.png
res/drawable-hdpi/make_focus.png
res/drawable-hdpi/make_head.png
res/drawable-hdpi/make_normal.png
res/drawable-hdpi/more_head.png
res/drawable-hdpi/new1.jpg
res/drawable-hdpi/new2.jpg
res/drawable-hdpi/new3.jpg
res/drawable-hdpi/new4.jpg
res/drawable-hdpi/new_hot.png

res/drawable-hdpi/new_middle1_n.png
res/drawable-hdpi/new_middle1_s.png
res/drawable-hdpi/new_middle2_n.png
res/drawable-hdpi/new_middle2_s.png
res/drawable-hdpi/new_middle3_n.png
res/drawable-hdpi/new_middle3_s.png
res/drawable-hdpi/new_middle4_n.png
res/drawable-hdpi/new_middle4_s.png
res/drawable-hdpi/new_new.png
res/drawable-hdpi/notice.png
res/drawable-hdpi/nowifi.png
res/drawable-hdpi/one.jpg
res/drawable-hdpi/ous.png
res/drawable-hdpi/ping.png
res/drawable-hdpi/qb.png
res/drawable-hdpi/rec_btn.png
res/drawable-hdpi/rec_btn_press.png
res/drawable-hdpi/search.png
res/drawable-hdpi/sebar_bg.png
res/drawable-hdpi/share.png
res/drawable-hdpi/small_bg.png
res/drawable-hdpi/star_empty.png
res/drawable-hdpi/star_selected.png
res/drawable-hdpi/test_app_icon.png
res/drawable-hdpi/test_app_image.png
res/drawable-hdpi/three.jpg
res/drawable-hdpi/titlebar_bg.png
res/drawable-hdpi/titlepage.jpg
res/drawable-hdpi/to.png
res/drawable-hdpi/two.jpg
res/drawable-hdpi/zhan.png
res/drawable-hdpi/zhifu.png
res/drawable-mdpi/ic_launcher.png
res/drawable-xhdpi/ic_launcher.png
res/drawable-xhdpi/img_coin.png
res/drawable-xxhdpi/ic_launcher.png
res/drawable/appdetbor.xml
res/drawable/bg_listview_item.xml
res/drawable/border.xml
res/drawable/button_download.xml
res/drawable/button_ex.xml
res/drawable/button_price.xml
res/drawable/button_title_back.xml
res/drawable/close_v.xml

res/drawable/home_btn_bg.xml
res/drawable/image_app_introduce.xml
res/drawable/image_app_reference.xml
res/drawable/listviewbg.xml
res/drawable/new_middle.xml
res/drawable/radius.xml
res/drawable/radiusbut1.xml
res/drawable/radiusbut2.xml
res/drawable/radiusbut3.xml
res/drawable/radiusbut4.xml
res/drawable/radiusbut5.xml
res/drawable/radiusbut6.xml
res/drawable/radiusbut7.xml
res/drawable/radiuss.xml
res/drawable/ratingbar_drawable.xml
res/layout-1280x768/news.xml
res/layout-1920x1080/news.xml
res/layout-960x540/news.xml
res/layout/app_detai_bar.xml
res/layout/app_detail.xml
res/layout/appstore.xml
res/layout/appstore_bar.xml
res/layout/appstore_listview.xml
res/layout/bg.xml
res/layout/close_view.xml
res/layout/dialog.xml
res/layout/dialog_qq.xml
res/layout/ding.xml
res/layout/exchange.xml
res/layout/float_view.xml
res/layout/item01.xml
res/layout/item02.xml
res/layout/item03.xml
res/layout/load.xml
res/layout/main.xml
res/layout/make_money.xml
res/layout/more.xml
res/layout/more_list.xml
res/layout/news.xml
res/layout/order_list.xml
res/layout/read.xml
res/layout/read_list.xml
res/layout/search.xml
res/layout/show.xml

res/layout/showhtml.xml
res/layout/showsearch.xml
res/layout/sitem.xml
res/menu/main.xml
resources.arsc
