MOBSF

ANDROID STATIC ANALYSIS REPORT

调皮女仆 (2.9.9)

File Name:	0b8bae30da84fb181a9ac2b1dbf77eddc5728fab8dc5db44c11069fef1821ae6.apk
Package Name:	com.ktdvau.myidglux
Scan Date:	May 21, 2023, 2:50 p.m.
App Security Score:	40/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	20	1	1	1

FILE INFORMATION

File Name: 0b8bae30da84fb181a9ac2b1dbf77eddc5728fab8dc5db44c11069fef1821ae6.apk
Size: 6.27MB
MD5: d65dcf5632685db88e2580ea34801d8c
SHA1: 3714c0906c11b24125c66441dd3d074cc99f2ee1
SHA256: 0b8bae30da84fb181a9ac2b1dbf77eddc5728fab8dc5db44c11069fef1821ae6

APP INFORMATION

App Name: 调皮女仆
Package Name: com.ktdvau.myidglux
Main Activity: org.cocos2dx.cpp.AppActivity
Target SDK: 9
Min SDK: 9
Max SDK:
Android Version Name: 2.9.9

Android Version Code: 4972

APP COMPONENTS

Activities: 7
Services: 13
Receivers: 3
Providers: 0
Exported Activities: 2
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=tv, ST=cn, L=te, O=vvygke, OU=upusos, CN=uvgiyq
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-01-22 20:47:46+00:00
Valid To: 2020-10-18 20:47:46+00:00
Issuer: C=tv, ST=cn, L=te, O=vvygke, OU=upusos, CN=uvgiyq
Serial Number: 0xef1228d
Hash Algorithm: sha256
md5: b82bb9f0fd4aecb0ee93ca4914aea76b
sha1: bd0947f41d478d3947ca474f4c95c6cf4cccdd87
sha256: ebe576b6edbd4571b5a91ff124a795e9e4f7d759c9a35347bc1729608ee28127
sha512: bd378284665e27dc525585cc3e7410fad5b3ba69dd77bf2221f28dacd5ecbeff8e03f9b21003c615746c5691a70e099cea4e8d3d020a025e34d74064d26148ce

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_SMS	dangerous	edit SMS or MMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.
android.permission.RECEIVE_USER_PRESENT	unknown	Unknown permission	Unknown permission from android reference
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.permission.DISABLE_KEYGUARD	normal		Allows applications to disable the keyguard if it is not secure.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	normal	access extra location provider commands	Access extra location provider commands. Malicious applications could use this to interfere with the operation of the GPS or other location sources.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
com.android.launcher.permission.UNINSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.SYSTEM_OVERLAY_WINDOW	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MOUNT_FORMAT_FILESYSTEMS	dangerous	format external storage	Allows the application to format removable storage.
android.permission.CHANGE_CONFIGURATION	SignatureOrSystem	change your UI settings	Allows an application to change the current configuration, such as the locale or overall font size.
android.permission.RUN_INSTRUMENTATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_MMS	dangerous	receive MMS	Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.RESTART_PACKAGES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.permission.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_WAP_PUSH	dangerous	receive WAP	Allows application to receive and process WAP messages. Malicious applications may monitor your messages or delete them without showing them to you.

APKID ANALYSIS

FILE	DETAILS
assets/dERlZG!classes.dex	FINDINGS: Compiler — DETAILS: dx
assets/jypaysdk.md!classes.dex	FINDINGS: Compiler — DETAILS: dx (possible dexmerge) FINDINGS: Manipulator Found — DETAILS: dexmerge
assets/wyzf/res.bin!classes.dex	FINDINGS: Compiler — DETAILS: dx

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>assets/yf/dynamiclib.bin!classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name check
device ID check
subscriber ID check
possible VM check</td></tr>
<tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 11 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=9]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
3	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (com.y.f.jar.pay.InNoticeReceiver) is not Protected. An intent-filter exists.	warning	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.
5	Broadcast Receiver (com.mn.kt.rs.RsRe) is not Protected. An intent-filter exists.	warning	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.
6	Service (com.mn.kt.rs.RsSe) is not Protected. An intent-filter exists.	warning	A Service 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 Service is explicitly exported.
7	Broadcast Receiver (com.comment.one.receiver.EBooReceiver) is not Protected. An intent-filter exists.	warning	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.
8	Service (com.yuanlang.pay.JobScheduleService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
9	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
10	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

NO	ISSUE	SEVERITY	DESCRIPTION
11	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
12	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 5 | WARNING: 8 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/c/a.java bn/sdk/szwcsss/codec/ab/Cfor.java bn/sdk/szwcsss/codec/ac/Cnew.java bn/sdk/szwcsss/codec/ag/Cif.java bn/sdk/szwcsss/codec/ai/Cbyte.java bn/sdk/szwcsss/codec/ai/Ccase.java bn/sdk/szwcsss/codec/ai/Cdo.java bn/sdk/szwcsss/codec/ai/Cgoto.java bn/sdk/szwcsss/codec/ak/Cif.java bn/sdk/szwcsss/codec/al/Cdo.java bn/sdk/szwcsss/codec/an/Cdo.java bn/sdk/szwcsss/codec/an/Cif.java bn/sdk/szwcsss/codec/an/Ctry.java bn/sdk/szwcsss/common/az/c/net/AbstractReq.java bn/sdk/szwcsss/common/az/c/net/Cbyte.java bn/sdk/szwcsss/common/az/c/net/Ccase.java bn/sdk/szwcsss/common/az/c/net/Cchar.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				bn/sdk/szwcsss/common/az/c/net/Cfo r.java bn/sdk/szwcsss/common/az/c/net/Cg oto.java bn/sdk/szwcsss/common/az/c/net/Cin t.java bn/sdk/szwcsss/common/az/c/net/Cn ew.java bn/sdk/szwcsss/common/az/c/net/Ctr y.java bn/sdk/szwcsss/common/az/c/pay/A.j ava bn/sdk/szwcsss/common/az/c/pay/Cd o.java bn/sdk/szwcsss/common/az/c/pay/Cf or.java bn/sdk/szwcsss/common/az/c/pay/Ctr y.java bn/sdk/szwcsss/common/az/c/service /Cdo.java bn/sdk/szwcsss/common/az/c/service /ServiceAction.java bn/sdk/szwcsss/common/az/code/b/C byte.java bn/sdk/szwcsss/common/az/code/b/C for.java bn/sdk/szwcsss/common/az/code/c/C do.java bn/sdk/szwcsss/common/az/code/c/C for.java bn/sdk/szwcsss/common/az/code/c/C goto.java bn/sdk/szwcsss/common/az/code/c/Ci f.java bn/sdk/szwcsss/common/kt/a/wc/d/Cf or.java bn/sdk/szwcsss/common/kt/a/wc/d/a. java bn/sdk/szwcsss/common/kt/a/wc/d/c.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	ava bn/sdk/szwcsss/common/kt/a/wc/d/d.java bn/sdk/szwcsss/common/kt/a/wc/d/e.java bn/sdk/szwcsss/common/y/Cint.java bn/sdk/szwcsss/common/y/Cnew.java bn/sdk/szwcsss/common/y/winit.java cn/cuter/main/Uncm.java com/amaz/onib/Utils.java com/amaz/onib/bb.java com/amaz/onib/bs.java com/amaz/onib/bu.java com/amaz/onib/cf.java com/amaz/onib/cq.java com/cocos/game/util/MyTallyUtil.java com/cocos/util/PLog.java com/cocos/util/SDcardUtil.java com/cocos/util/Tools.java com/dataeye/c/x.java com/jy/a/b.java com/jy/a/e.java com/jy/publics/JyActivity.java com/jy/publics/JyPaySDKMain.java com/jy/publics/ReceiverUtil.java com/jy/publics/service/JyService.java com/jy/utils/InitConfigPro.java com/jy/utils/LOG.java com/mn/kt/c/b/a.java com/mobile/bumptech/ordinary/miniSDK/SDK/b/b.java com/mobile/bumptech/ordinary/miniSDK/SDK/b/d.java com/mobile/bumptech/ordinary/miniSDK/SDK/c/h.java com/mobile/bumptech/ordinary/miniSDK/SDK/intf/MApplication.java com/mobile/bumptech/ordinary/miniSDK/SDK/intf/StatService.java com/mobile/bumptech/ordinary/miniSDK/SDK/intf/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mobile/bumptech/ordinary/miniSDK/SDK/intf/event/MobclickAgent.java com/mobile/bumptech/ordinary/miniSDK/SDK/intf/util/a.java com/payment/plus/c/g.java com/payment/plus/c/k.java com/payment/plus/c/m.java com/payment/plus/d/a.java com/payment/plus/d/b.java com/payment/plus/d/c.java com/payment/plus/d/d.java com/payment/plus/d/e.java com/payment/plus/d/f.java com/payment/plus/d/g.java com/payment/plus/sk/abcdef/jczdf/b/b.java com/payment/plus/sk/abcdef/jczdf/b/d.java com/payment/plus/sk/abcdef/jczdf/c/h.java com/payment/plus/sk/abcdef/jczdf/c/l.java com/payment/plus/sk/abcdef/jczdf/intf/MApplication.java com/payment/plus/sk/abcdef/jczdf/intf/StatService.java com/payment/plus/sk/abcdef/jczdf/intf/c.java com/payment/plus/sk/abcdef/jczdf/intf/event/MobclickAgent.java com/payment/plus/sk/abcdef/jczdf/intf/util/a.java com/umeng/analytics/pro/by.java com/wyzfpay/a/a.java com/wyzfpay/b/a.java com/wyzfpay/net/AbstractReq.java com/wyzfpay/util/LogUtils.java com/wyzfpay/util/a.java com/wyzfpay/util/e.java com/yf/y/f/init/download/SdkDlm.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/yf/y/f/init/http/HttpUtil.java com/yf/y/f/init/http/UploadUtil.java com/yf/y/f/init/multidex/WyzfDex.java com/yf/y/f/init/net/AbstractReq.java com/yf/y/f/init/pay/SZYTPay.java com/yf/y/f/init/service/InitService.java com/yf/y/f/init/util/Base64.java com/yf/y/f/init/util/CustomLog.java com/yf/y/f/init/util/DesUtil.java com/yf/y/f/init/util/LogUtils.java org/cocos2dx/cpp/AppActivity.java org/cocos2dx/lib/Cocos2dxActivity.java org/cocos2dx/lib/Cocos2dxBitmap.java org/cocos2dx/lib/Cocos2dxGLSurfaceView.java org/cocos2dx/lib/Cocos2dxHttpURLConnection.java org/cocos2dx/lib/Cocos2dxLocalStorage.java org/cocos2dx/lib/Cocos2dxMusic.java org/cocos2dx/lib/Cocos2dxSound.java org/cocos2dx/lib/Cocos2dxVideoView.java org/cocos2dx/lib/Cocos2dxWebView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	bn/sdk/szwcsss/codec/ac/Cif.java bn/sdk/szwcsss/codec/ac/Cnew.java bn/sdk/szwcsss/codec/ag/Cif.java bn/sdk/szwcsss/codec/ah/Cfor.java bn/sdk/szwcsss/codec/x/Cdo.java bn/sdk/szwcsss/common/az/code/c/Cint.java com/cocos/util/FileUtil.java com/cocos/util/PLog.java com/cocos/util/SDcardUtil.java com/cocos/util/StorageUtil.java com/cocos/util/Tools.java com/dataeye/c/af.java com/dataeye/c/x.java com/jy/a/b.java com/jy/utils/LOG.java com/mn/kt/d/a.java com/mobile/bumptech/ordinary/miniSDK/SDK/a/b.java com/mobile/bumptech/ordinary/miniSDK/SDK/c/h.java com/mobile/bumptech/ordinary/miniSDK/SDK/c/o.java com/payment/plus/sk/abcdef/jczdf/a/b.java com/payment/plus/sk/abcdef/jczdf/c/h.java com/payment/plus/sk/abcdef/jczdf/c/p.java com/umeng/analytics/pro/am.java com/wyzfpay/util/LogUtils.java com/yf/y/f/init/constant/Constant.java com/yf/y/f/init/util/CrashHandler.java com/yf/y/f/init/util/LogUtils.java com/yuanlang/pay/plugin/libs/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	bn/sdk/szwcsss/codec/ac/Ctry.java bn/sdk/szwcsss/codec/ah/Cif.java bn/sdk/szwcsss/codec/am/Cdo.java bn/sdk/szwcsss/common/az/code/c/Cfor.java com/amaz/onib/ck.java com/comment/one/e/b.java com/dataeye/c/ai.java com/mn/kt/d/a.java com/payment/plus/b/a.java com/wyzfpay/util/e.java com/yf/y/f/init/util/DesUtil.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/umeng/analytics/pro/an.java com/umeng/analytics/pro/ao.java org/cocos2dx/lib/Cocos2dxHttpURLConnection.java
5	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/amaz/onib/cl.java com/cocos/game/pay/SA_Pay.java com/umeng/analytics/pro/an.java com/yf/y/f/init/util/ConstUtils.java com/yf/y/f/init/util/DesUtil.java org/cocos2dx/cpp/AppActivity.java org/cocos2dx/cpp/MyApplication.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	a/b/a.java bn/sdk/szwcsss/common/az/code/a/Cdo.java com/amaz/onib/g.java com/dataeye/c/p.java com/dataeye/c/u.java com/dataeye/c/v.java com/mn/kt/c/a/a.java com/mn/kt/c/a/b.java com/mn/kt/c/b/a.java com/umeng/analytics/pro/a.java com/umeng/analytics/pro/c.java com/umeng/analytics/pro/t.java com/umeng/analytics/pro/v.java com/umeng/analytics/pro/w.java org/cocos2dx/lib/Cocos2dxLocalStorage.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	a/a/b.java a/e/d.java a/e/e.java bn/sdk/szwcsss/codec/ac/Ccase.java com/amaz/onib/bg.java com/amaz/onib/bk.java com/amaz/onib/bt.java com/amaz/onib/by.java com/amaz/onib/bz.java com/amaz/onib/ck.java com/amaz/onib/cm.java com/amaz/onib/cq.java com/comment/one/c/b.java com/dataeye/c/af.java com/jy/a/b.java com/jy/utils/MD5Encoder.java com/mn/kt/d/a.java com/payment/plus/c/a.java com/umeng/analytics/pro/bt.java com/umeng/analytics/pro/bv.java com/umeng/analytics/pro/bw.java com/wyzfpay/util/f.java com/yf/y/f/init/util/FileUtils.java org/cocos2dx/cpp/MyUtils.java
8	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	a/e/d.java cn/cuter/main/Uncm.java com/amaz/onib/Utils.java com/amaz/onib/bk.java com/amaz/onib/bl.java com/amaz/onib/v.java com/dataeye/c/a.java com/umeng/analytics/pro/bt.java com/umeng/analytics/social/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/amaz/onib/bk.java
10	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	a/a/b.java bn/sdk/szwcsss/common/az/code/c/Cfor.java com/dataeye/c/ai.java com/umeng/analytics/pro/bt.java com/wyzfpay/util/e.java com/yf/y/f/init/util/DesUtil.java
11	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/amaz/onib/bj.java com/amaz/onib/bm.java com/amaz/onib/bn.java com/amaz/onib/bo.java
12	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/umeng/analytics/pro/bt.java
13	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	bn/sdk/szwcsss/codec/ad/Ctry.java com/dataeye/c/af.java com/umeng/analytics/pro/aw.java
14	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	bn/sdk/szwcsss/codec/ad/Ctry.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/comment/one/e/a.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi/libbsjni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi/libcrypt_sign.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
3	lib/armeabi/libgirlstar_v2.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'location'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['system logs'].
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
12	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
13	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
14	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
15	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
16	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
18	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
19	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
m.miguxue.com	ok	**IP:** 185.53.177.52 **Country:** Germany **Region:** Bayern **City:** Munich **Latitude:** 48.137428 **Longitude:** 11.575490 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
192.168.10.194	ok	**IP:** 192.168.10.194 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
client.cmread.com	ok	**IP:** 211.140.17.83 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
cf.gdatacube.net	ok	No Geolocation information available.
www.zhjnn.com	ok	No Geolocation information available.
alog.umengcloud.com	ok	**IP:** 8.211.35.113 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
wap.cmread.com	ok	**IP:** 211.140.17.81 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
vpay.api.eerichina.com	ok	No Geolocation information available.
139.129.132.111	ok	**IP:** 139.129.132.111 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
uop.umeng.com	ok	No Geolocation information available.
120.26.106.206	ok	**IP:** 120.26.106.206 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.baidu.com	ok	**IP:** 103.235.46.40 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
118.85.194.4	ok	**IP:** 118.85.194.4 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
wap.tyread.com	ok	**IP:** 220.187.224.30 **Country:** China **Region:** Zhejiang **City:** Shaoxing **Latitude:** 30.011021 **Longitude:** 120.571533 **View:** Google Map
xixi.dj111.top	ok	No Geolocation information available.
alog.umeng.com	ok	**IP:** 8.211.36.31 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pay.918ja.com	ok	**IP:** 112.124.36.43 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
sdk.qipagame.cn	ok	No Geolocation information available.
cmnsguider.yunos.com	ok	**IP:** 203.119.175.203 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
web.5ayg.cn	ok	No Geolocation information available.
121.40.109.196	ok	**IP:** 121.40.109.196 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
10.235.148.9	ok	**IP:** 10.235.148.9 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
log.umsns.com	ok	**IP:** 59.82.29.249 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
biss.cmread.com	ok	**IP:** 211.140.17.120 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
pay.5ayg.cn	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

Report Generated by - MobSF v3.6.7 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.