APP SCORES

Security Score 42/100

Trackers Detection 11/432

FILE INFORMATION

File Name com.benqu.wuta_6.5.5.151-655_minAPI21_arm64-v8a_armeabi-v7a_nodpi_apkmirror.com.apk

Size 99.8MB

MD5 c2bf6519e2c41f262e8de0b3cd4e0b21

SHA1 4bb06bb8a65485f6b2ff0cf73ce54f5324ece662

SHA256 68be7514c3dc0b511ef313a90b5f1e9cd03884af0e02c7c4588ba3b971677244

APP INFORMATION

App Name Wuta Cam

Package Name com.benqu.wuta

Main Activity com.benqu.wuta.activities.splash.SplashActivity

Target SDK 34 **Min SDK** 21 **Max SDK**

Android Version Name 6.5.5.151 **Android Version Code** 655

PLAYSTORE INFORMATION

Title Wuta Camera - Nice Shot Always

Score 4.23 **Installs** 10,000,000+ **Price** 0 **Android Version Support** **Category** Photography **Play Store URL** com.benqu.wuta

Developer Benqu, **Developer ID** 5164337428081395139

Developer Address Room 1101, No. 100, Qinzhou Road, Xuhui District, Shanghai

Developer Website https://www.wuta-cam.com/

Developer Email develop@wuta-camera.com

Release Date Jan 18, 2017 **Privacy Policy** Privacy link

Description

```
All-round camera app, natural, high-quality, and clear are its characteristics.

Known and praised widely by more than 200 million users.

Wuta Camera, nice shot always!


[Cosmetic Medical Facial Edit]
New “3D Rhinoplasty” comes online! From the root of nose, the bridge of nose, the ala of nose to the tip of nose, beautify your nose in high-quality multi dimension. Make you have a natural, tall and strong nose easily, at the same time with other facial features perfect fit!
More than 20 other beauty functions edit your face to make it look more beautiful and natural at the same time.

[Best Skin Texture Template]
Best skin texture template comes online! There are 7 skin styles to choose, which are classic, soft, cream, soft foggy, original, texture, men style. Having model face in one click, more choose more beautiful.

[Special sticker style]
Collect of the latest, good-looking and most fun style stickers, including many features, style filters, personality selfie elements. Keep up with the trend of the times, go with the fashion.

[4D Original Makeup]
Super lifelike makeup effect, without fear of all kinds of angles, all kinds of expressions, even when you are makeup-free, retouch skin tone using our exclusive skin smoothing tool with our camera.

[Sketch Art Editor]
Sketch function in direct shooting, color lead/black and white arbitrary switch.
```

10 / 140
EXPORTED ACTIVITIES
View All

10 / 34
EXPORTED SERVICES
View All

6 / 22
EXPORTED RECEIVERS
View All

1 / 13
EXPORTED PROVIDERS
View All

SCAN OPTIONS **DECOMPILED CODE**

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=086, ST=Shanghai, L=Shanghai, O=上海本趣网络科技有限公司, OU=Benqumark, CN=Benqumark
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-06-17 03:47:14+00:00
Valid To: 2116-05-24 03:47:14+00:00
Issuer: C=086, ST=Shanghai, L=Shanghai, O=上海本趣网络科技有限公司, OU=Benqumark, CN=Benqumark
Serial Number: 0x66f1525e
Hash Algorithm: sha256
md5: 50590c0e714e943053ebb79765b544a3
sha1: 86883db0d90d09e42298aaf27bf2d44fd8aa171e
sha256: df195732442966b578d581fe346792974cc6c220964c9e61cd47366e3b5332a1
sha512: 885f3853d35298d65a03e600d10c483280530a70fcab87e5a3abf7a74f924cd1c5990e686165a3d2261fc94a31791164c8a9ac1bacf361c0a921ed7c1c35cd9b
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 41c4a694464dfb66c06bf4b5181cb84db07278f41aa2dbb4d8ce77baad10e8a6
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.	
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.	
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.	
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.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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.	
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.	
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.	

Showing 1 to 10 of 53 entries

Previous 1 2 3 4 5 6 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	

API	FILES
Certificate Handling	
Content Provider	
Crypto	
Dynamic Class and Dexloading	
Execute OS Command	
Get Android Advertising ID	
Get Cell Information	

Showing 1 to 10 of 46 entries

Previous 1 2 3 4 5 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
com.benqu.upush.VendorMsgClickActivity	**Schemes**: agoo://, **Hosts:** com.benqu.wuta, **Paths:** /thirdpush,
com.benqu.wuta.activities.splash.SplashActivity	**Schemes**: wuta_cam://, wuta://, **Hosts:** record, photograph, action,

ACTIVITY	INTENT
com.tencent.tauth.AuthActivity	**Schemes**: tencent101912038://,

Showing 1 to 3 of 3 entries

Previous 1 Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
2	1	0	0

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.

Showing 1 to 3 of 3 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	1	1

Search:

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	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.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 2 of 2 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
2	29	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.	
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	
4	**Service** (com.benqu.wuta.activities.vcam.VcamService) is not Protected. [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.	
5	**Activity** (com.benqu.wuta.wxapi.WXPayEntryActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
6	**Broadcast Receiver** (com.just.agentweb.RealDownLoader$NotificationBroadcastReceiver) is not Protected. [android:exported=true]	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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
7	**Activity** (com.benqu.upush.VendorMsgClickActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
8	**Broadcast Receiver** (com.benqu.upush.VendorMZMsgReceiver) is not Protected. [android:exported=true]	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.	
9	**Service** (com.heytap.msp.push.service.CompatibleDataMessageCallbackService) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.coloros.mcs.permission.SEND_MCS_MESSAGE [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.	
10	**Service** (com.heytap.msp.push.service.DataMessageCallbackService) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.heytap.mcs.permission.SEND_PUSH_MESSAGE [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.	

Showing 1 to 10 of 34 entries

Previous 1 2 3 4 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
6	10	2	2	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	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		
2	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		
3	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		
4	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		
5	IP Address disclosure	warning	**CWE:** CWE-200: Information Exposure **OWASP MASVS:** MSTG-CODE-2		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
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		
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4		
8	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		
9	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		
10	App creates temp file. Sensitive information should never be written into a temp file.	warning	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2		

Showing 1 to 10 of 20 entries

Previous 1 2 Next

SHARED LIBRARY BINARY ANALYSIS

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libwtcore.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**True** info The binary has the following fortified functions: ['__umask_chk']	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libmmkv.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**True** info The binary has the following fortified functions: ['__vsnprintf_chk', '__strchr_chk', '__strcat_chk', '__memcpy_chk', '__read_chk', '__strncpy_chk']	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi-v7a/ libst_mobile.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Partial RELRO** warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**True** info The binary has the following fortified functions: ['__FD_SET_chk']	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	armeabi-v7a/ libapminsighta.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary 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. This check is not applicable for Dart/Flutter libraries.	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/ libzmedia_native.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**True** info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libglide-webp.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary 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. This check is not applicable for Dart/Flutter libraries.	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/ libtobEmbedPagEncrypt.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary 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. This check is not applicable for Dart/Flutter libraries.	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	armeabi-v7a/ libshadowhook.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary 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. This check is not applicable for Dart/Flutter libraries.	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi-v7a/libc++_shared.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary 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. This check is not applicable for Dart/Flutter libraries.	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/ libwtmedia.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary 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.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary 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. This check is not applicable for Dart/Flutter libraries.	**True** info Symbols are stripped.

Showing 1 to 10 of 112 entries

Previous 1 2 3 4 5 ... 12 Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
1	Hardcoded Keystore found.	assets/grs_sp.bks assets/hmsincas.bks assets/hmsrootcas.bks

Showing 1 to 1 of 1 entries

Previous 1 Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS
assets/audience_network.dex	Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Compiler	unknown (please file detection issue!)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check device ID check subscriber ID check ro.product.device check ro.kernel.qemu check emulator file check
Compiler	r8

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes2.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.MANUFACTURER check network operator name check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes3.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.MANUFACTURER check Build.BOARD check network operator name check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes4.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check SIM operator check subscriber ID check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes5.dex	Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check SIM operator check
Compiler	r8 without marker (suspicious)

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes6.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes7.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check SIM operator check network operator name check subscriber ID check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes8.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.MANUFACTURER check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
lib/arm64-v8a/libst_mobile.so	Search:

FINDINGS	DETAILS
Obfuscator	Obfuscator-LLVM version unknown

Showing 1 to 1 of 1 entries

Previous 1 Next

Showing 1 to 10 of 12 entries

Previous 1 2 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	
00002	Open the camera and take picture	camera	com/bhs/zcam/cam1/Cam1Device.java
00003	Put the compressed bitmap data into JSON object	camera	com/tencent/connect/avatar/ImageActivity.java com/umeng/message/proguard/ag.java
00004	Get filename and put it to JSON object	file collection	
00005	Get absolute path of file and put it to JSON object	file	

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java
00012	Read data and put it into a buffer stream	file	
00013	Read file and put it into a stream	file	

Showing 1 to 10 of 71 entries

Previous 1 2 3 4 5 … 8 Next

ABUSED PERMISSIONS

Top Malware Permissions **12**/25

android.permission.CAMERA,
android.permission.RECORD_AUDIO,
android.permission.ACCESS_COARSE_LOCATION,
android.permission.ACCESS_FINE_LOCATION,
android.permission.ACCESS_NETWORK_STATE,
android.permission.ACCESS_WIFI_STATE,
android.permission.INTERNET,
android.permission.WRITE_EXTERNAL_STORAGE,
android.permission.WAKE_LOCK,
android.permission.GET_TASKS,
android.permission.READ_EXTERNAL_STORAGE,
android.permission.VIBRATE

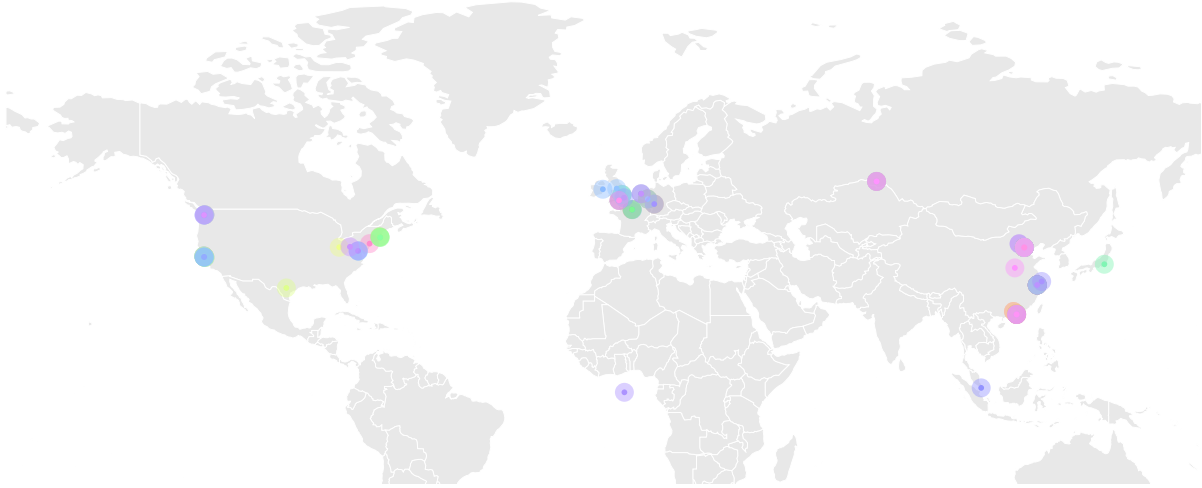
Other Common Permissions **6**/44

android.permission.FLASHLIGHT, android.permission.FOREGROUND_SERVICE,
android.permission.CHANGE_WIFI_STATE,
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE,
com.google.android.c2dm.permission.RECEIVE,
com.google.android.gms.permission.AD_ID

Malware Permissions are the top permissions that are widely abused by known malware.

Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS



This app may communicate with the following OFAC sanctioned list of countries.

Search:

DOMAIN	COUNTRY/REGION

DOMAIN	COUNTRY/REGION
8.136.104.193	**IP:** 8.136.104.193 **Country:** China **Region:** Zhejiang **City:** Hangzhou
ad.tmsdk.cn	**IP:** 114.250.48.245 **Country:** China **Region:** Beijing **City:** Beijing
admin-debug.wuta-cam.com	**IP:** 139.224.69.31 **Country:** China **Region:** Zhejiang **City:** Hangzhou
admin-release.wuta-cam.com	**IP:** 139.224.69.31 **Country:** China **Region:** Zhejiang **City:** Hangzhou
ai-api-release.wuta-cam.com	**IP:** 47.97.186.237 **Country:** China **Region:** Zhejiang **City:** Hangzhou
api-debug.wuta-cam.com	**IP:** 47.101.210.193 **Country:** China **Region:** Zhejiang **City:** Hangzhou

DOMAIN	COUNTRY/REGION
api-push.meizu.com	**IP:** 14.152.79.165 **Country:** China **Region:** Guangdong **City:** Guangzhou
api-release.wuta-cam.com	**IP:** 47.243.165.222 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong
api.ssp.zxrtb.com	**IP:** 39.97.130.98 **Country:** China **Region:** Zhejiang **City:** Hangzhou
api.weibo.com	**IP:** 36.51.224.49 **Country:** China **Region:** Beijing **City:** Beijing

Showing 1 to 10 of 53 entries

Previous 1 2 3 4 5 6 Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
10.38.162.35	ok	**IP:** 10.38.162.35 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
8.136.104.193	ok	**IP:** 8.136.104.193 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
aa.unioneeu.com	ok	**IP:** 13.250.183.62 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
ad.tmsdk.cn	ok	**IP:** 114.250.48.245 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
admin-debug.wuta-cam.com	ok	**IP:** 139.224.69.31 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
admin-release.wuta-cam.com	ok	**IP:** 139.224.69.31 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
ai-api-release.wuta-cam.com	ok	**IP:** 47.97.186.237 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
alogsus.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
alogus.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
analytics.wuta-cam.com	ok	No Geolocation information available.

Showing 1 to 10 of 124 entries

Previous 1 2 3 4 5 … 13 Next

URLS

Search:

URL	FILE
data:application/mpeg4-bifs-au;base64,%s data:application/mpeg4-iod;base64,%s data:application/mpeg4-od-au;base64,%s	apktool_out/lib/arm64-v8a/libwtmedia.so
data:application/mpeg4-bifs-au;base64,%s data:application/mpeg4-iod;base64,%s data:application/mpeg4-od-au;base64,%s	lib/arm64-v8a/libwtmedia.so
data:application/mpeg4-bifs-au;base64,%s data:application/mpeg4-od-au;base64,%s	apktool_out/lib/armeabi-v7a/libwtmedia.so

URL	FILE
data:application/mpeg4-bifs-au;base64,%s data:application/mpeg4-od-au;base64,%s	lib/armeabi-v7a/libwtmedia.so
data:b}};function data:d,underevaluation:c}):c=null;if(null==c)break;hc(a.g,b,c,!1);break;case data:this.context_.customreferencedata, data:b}));return!0};function data:d},c)}function	com/vungle/ads/internal/omsdk/Res.java
data:d},c)}function data:a.data}};function	com/bytedance/sdk/openadsdk/core/QQr/XD.java
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
 data:text/csv;charset=utf-8,	com/just/agentweb/RealDownLoader.java
data:text/csv;	com/just/agentweb/DefaultDownloadImpl.java
data:text/html	com/bytedance/sdk/component/widget/SSWebView.java

Showing 1 to 10 of 227 entries

Previous 1 2 3 4 5 … 23 Next

EMAILS

Search:

EMAIL	FILE
support@wuta-camera.com	com/benqu/wuta/activities/setting/FeedbackActivity.java
可以通过人工客服或发邮件至support@wuta-camera.com与我们联系 support@wuta-camera.com	Android String Resource

Showing 1 to 2 of 2 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Baidu Mobile Ads		https://reports.exodus-privacy.eu.org/trackers/100
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328

TRACKER NAME	CATEGORIES	URL
Mintegral	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/200
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

Showing 1 to 10 of 11 entries

Previous 1 2 Next

POSSIBLE HARDCODED SECRETS

▸ Show all **3247** secrets

STRINGS

From APK Resource

▸ Show all **11170** strings

From Code

▸ Show all **78102** strings

From Shared Objects

apktool_out/lib/armeabi-v7a/libwtcore.so

▸ Show all **9558** strings

apktool_out/lib/armeabi-v7a/libmmkv.so