⭐ Security Score

42

Security Score 42/100

🎛 Risk Rating

Medium Risk

Grade

| A | **B** | C | F |

🥧 Severity Distribution (%)

■ High ■ Medium ■ Info ■ Secure

🛍 Privacy Risk

11

User/Device Trackers

📄 Findings

| 🐞 | High **11** | | ⚠️ | Medium **42** |

| ℹ️ | Info **2** | | ✅ | Secure **2** |

| 🔍 | Hotspot **51** | | | |

`high` Base config is insecurely configured to permit clear text traffic to all domains **NETWORK**

`high` Base config is configured to trust user installed certificates **NETWORK**

`high` App can be installed on a vulnerable unpatched Android version **MANIFEST**

`high` Clear text traffic is Enabled For App **MANIFEST**

`high` The file or SharedPreference is World Writable. Any App can write to the file **CODE**

`high` The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks. **CODE**

`high` 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. **CODE**

`high` Remote WebView debugging is enabled. **CODE**

`high` Weak Encryption algorithm used **CODE**

`high` 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 **CODE**

`high` Application contains Privacy Trackers **TRACKERS**

`medium` Application vulnerable to Janus Vulnerability **CERTIFICATE**

`medium` Base config is configured to trust system certificates **NETWORK**

`medium` Service (com.benqu.wuta.activities.vcam.VcamService) is not Protected. **MANIFEST**

`medium` Activity (com.benqu.wuta.wxapi.WXPayEntryActivity) is not Protected. **MANIFEST**

`medium` Broadcast Receiver (com.just.agentweb.RealDownLoader$NotificationBroadcastReceiver) is not Protected. **MANIFEST**

`medium` Activity (com.benqu.upush.VendorMsgClickActivity) is not Protected. **MANIFEST**

`medium` Broadcast Receiver (com.benqu.upush.VendorMZMsgReceiver) is not Protected. **MANIFEST**

`medium` Service (com.heytap.msp.push.service.CompatibleDataMessageCallbackService) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

`medium` Service (com.heytap.msp.push.service.DataMessageCallbackService) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

`medium` Activity (com.sina.weibo.sdk.share.ShareResultActivity) is not Protected. **MANIFEST**

`medium` TaskAffinity is set for activity **MANIFEST**

`medium` Activity (com.benqu.wuta.wxapi.WXEntryActivity) is not Protected. **MANIFEST**

`medium` Activity (com.tencent.tauth.AuthActivity) is not Protected. **MANIFEST**

`medium` Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

`medium` Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

`medium` Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

`medium` Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

`medium` Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

`medium` TaskAffinity is set for activity **MANIFEST**

`medium` Activity-Alias (com.umeng.message.UMessageNotifyActivity) is not Protected. **MANIFEST**

`medium` Service (com.taobao.accs.data.MsgDistributeService) is not Protected. **MANIFEST**

`medium` Broadcast Receiver (org.android.agoo.xiaomi.MiPushBroadcastReceiver) is not Protected. **MANIFEST**

`medium` Service (com.xiaomi.mipush.sdk.PushMessageHandler) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

`medium` Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) is not Protected. **MANIFEST**

`medium` Service (com.huawei.hms.support.api.push.service.HmsMsgService) is not Protected. **MANIFEST**

`medium` Content Provider (com.huawei.hms.support.api.push.PushProvider) is not Protected. **MANIFEST**

`medium` Service (com.meizu.cloud.pushsdk.NotificationService) is not Protected. **MANIFEST**

`medium` Service (com.vivo.push.sdk.service.CommandClientService) is not Protected. **MANIFEST**

`medium` Activity (com.sina.weibo.sdk.share.ShareTransActivity) is not Protected. **MANIFEST**

`medium` Activity (com.alipay.sdk.app.PayResultActivity) is not Protected. **MANIFEST**

`medium` Activity (com.alipay.sdk.app.AlipayResultActivity) is not Protected. **MANIFEST**

`medium` App can read/write to External Storage. Any App can read data written to External Storage. **CODE**

`medium` Files may contain hardcoded sensitive information like usernames, passwords, keys etc. **CODE**

`medium` The App uses an insecure Random Number Generator. **CODE**

`medium` 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. **CODE**

`medium` IP Address disclosure **CODE**

`medium` SHA-1 is a weak hash known to have hash collisions. **CODE**

`medium` MD5 is a weak hash known to have hash collisions. **CODE**

`medium` Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. **CODE**

`medium` Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system. **CODE**

`medium` App creates temp file. Sensitive information should never be written into a temp file. **CODE**

`medium` This app may contain hardcoded secrets **SECRETS**

`info` The App logs information. Sensitive information should never be logged. **CODE**

`info` This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it. **CODE**

`secure` This App may have root detection capabilities. **CODE**

`secure` This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. **CODE**

`hotspot` Found 11 critical permission(s) **PERMISSIONS**

`hotspot` App may communicate to a server (log.wuta-cam.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (res-debug.wuta-cam.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (api.ssp.zxrtb.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (pslog.umeng.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (ccs.umeng.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (mp.weixin.qq.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (openmobile.qq.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (audid.umeng.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (loggw-exsdk.alipay.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (log-debug.wuta-cam.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (pitk.unioneeu.com) in OFAC sanctioned country (Hong Kong) **DOMAINS**

`hotspot` App may communicate to a server (errnewlog.umeng.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (mobilegw.alipaydev.com) in OFAC sanctioned country (Hong Kong) **DOMAINS**

`hotspot` App may communicate to a server (service.weibo.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (api-push.meizu.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (aspect-upush.umeng.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (admin-debug.wuta-cam.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (errlog.umeng.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (open.weibo.cn) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (developer.umeng.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (msg.umengcloud.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (appsupport.qq.com) in OFAC sanctioned country (China) **DOMAINS**

`hotspot` App may communicate to a server (ucc.umeng.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (api-debug.wuta-cam.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (weibo.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (ulogs.umengcloud.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (ad.tmsdk.cn) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (admin-release.wuta-cam.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (offmsg.umeng.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (sss.umeng.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (h.trace.qq.com) in OFAC sanctioned country (Hong Kong)

DOMAINS

`hotspot` App may communicate to a server (mobilegw.alipay.com) in OFAC sanctioned country (Hong Kong)

DOMAINS

`hotspot` App may communicate to a server (errlogos.umeng.com) in OFAC sanctioned country (Hong Kong)

DOMAINS

`hotspot` App may communicate to a server (mobilegwpre.alipay.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (8.136.104.193) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (errnewlogos.umeng.com) in OFAC sanctioned country (Hong Kong)

DOMAINS

`hotspot` App may communicate to a server (mobilegw.dl.alipaydev.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (www.baidu.com) in OFAC sanctioned country (Hong Kong)

DOMAINS

`hotspot` App may communicate to a server (imgcache.qq.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (ai-api-release.wuta-cam.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (plbslog.umeng.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (open.weixin.qq.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (ulogs.umeng.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (api.weibo.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (cgi.connect.qq.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (norma-external-collect.meizu.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (statist.tingmall.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (utoken.umeng.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (long.open.weixin.qq.com) in OFAC sanctioned country (China)

DOMAINS

`hotspot` App may communicate to a server (ssapi.mosspf.com) in OFAC sanctioned country (Hong Kong)

DOMAINS

MobSF Application Security Scorecard generated for 無 (Wuta Cam 6.5.5.151) 🤖