# ANDROID STATIC ANALYSIS REPORT

## AndTTT (0.6.2)

| | |
|---|---|
| File Name: | installer203.apk |
| Package Name: | com.github.dawidd6.andttt |
| Scan Date: | May 31, 2022, 8:19 a.m. |
| App Security Score: | 55/100 (MEDIUM RISK) |
| Grade: | B |

## FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 1 | 2 | 1 | 1 | 0 |

## FILE INFORMATION

**File Name:** installer203.apk
**Size:** 1.22MB
**MD5:** b6aacb652f71dd10b185d2c887d7acf6
**SHA1:** dac012006cf9802c34f54bc1f36108eeda3f9557
**SHA256:** 3382ef9f021cfa799bea8b1372830d1f5ff7fbbccd136f72e88ac8892663ac36

## APP INFORMATION

**App Name:** AndTTT
**Package Name:** com.github.dawidd6.andttt
**Main Activity:** com.github.dawidd6.andttt.activities.MainActivity
**Target SDK:** 28
**Min SDK:** 21
**Max SDK:**
**Android Version Name:** 0.6.2
**Android Version Code:** 62

# APP COMPONENTS

**Activities:** 2
**Services:** 1
**Receivers:** 0
**Providers:** 0
**Exported Activities:** 0
**Exported Services:** 0
**Exported Receivers:** 0
**Exported Providers:** 0

# CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-01 08:07:48+00:00
Valid To: 2048-03-19 08:07:48+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x22490452ea418781
Hash Algorithm: sha256
md5: 27f20f624de0e8578b6eca4d8c424e42
sha1: eba6cfc10e51684eae24d4f0d0bd961f066a3921
sha256: b1e391e0a3a89e387359d494e9674e94b0cfd9ec0afa15b4ad41013a09eab893
sha512: e709e0cfd65f5e3e8bfb9ec839dcafcb0a8475fcd1c142edca61c927f0be1fe4dec1ab221355738eab79fae310d0a809c8086fc9dc14f26c2b26d5de08f5b9ba
```

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Signed Application | info | Application is signed with a code signing certificate |

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| 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. |

## APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |

## APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

## NETWORK SECURITY

| NO | SCOPE | SEVERITY | DESCRIPTION |
|---|---|---|---|

## MANIFEST ANALYSIS

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | Application Data can be Backed up [android:allowBackup=true] | warning | 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. |

## CODE ANALYSIS

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|

| 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<br>OWASP MASVS: MSTG-STORAGE-3 | me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java<br>butterknife/ButterKnife.java<br>a/a/c/a/e.java<br>a/a/c/c/b.java<br>a/a/c/b/b/b.java<br>a/a/c/c/i/e.java<br>a/a/c/c/h.java<br>a/a/d/e/d.java<br>a/a/c/c/f.java<br>a/a/c/c/i/a.java<br>a/a/c/h/f.java<br>a/a/c/h/c.java<br>a/a/b/a/i.java<br>a/a/c/h/q.java<br>a/a/c/c/e.java<br>a/a/c/h/p.java<br>com/afollestad/materialdialogs/internal/c.java<br>me/zhanghai/android/materialprogressbar/MaterialProgressBar.java<br>a/a/d/b/a/b.java<br>a/a/c/a/f.java |
| 2 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | b/b/a/a/d/b.java<br>b/b/a/a/c/d.java<br>b/b/a/a/d/c.java<br>b/b/a/a/d/d.java<br>b/b/a/a/c/c.java<br>b/b/a/a/c/b.java<br>b/b/a/a/f/a.java |

## NIAP ANALYSIS v1.3

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 1 | FCS_RBG_EXT.1.1 | Security Functional Requirements | Random Bit Generation Services | The application use no 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']. |
| 5 | FDP_DEC_EXT.1.2 | Security Functional Requirements | Access to Platform Resources | The application has access to no sensitive information repositories. |
| 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 does not encrypt files 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. |

## DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| github.com | ok | **IP:** 140.82.121.4<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| android.googlesource.com | ok | **IP:** 142.250.27.82<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| schemas.android.com | ok | No Geolocation information available. |

## Report Generated by - MobSF v3.5.2 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.