ANDROID STATIC ANALYSIS REPORT

AndTTT (0.6.2)

File Name:	installer158.apk
Package Name:	com.github.dawidd6.andttt
Scan Date:	May 30, 2022, 3:52 p.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	4	1	1	0

FILE INFORMATION

File Name: installer158.apk
Size: 1.45MB
MD5: 08c1dbbf7819772abeb624245a89beca
SHA1: 526712e5b7c184a22cf241e2cd9f6a2e6a799102
SHA256: 47e96271351d23009f1db722c0fd527ed466210c802bf2fecfba9d50891b5570

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: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-10-23 16:18:50+00:00
Valid To: 2050-10-16 16:18:50+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: a083cd30104cc84716b30253d051cc2b
sha1: d8650de9d663660bbb98cef312f5466c5234f2a7
sha256: 792b64e7343ef4dccd6f200f4fb4ba5b38b19e266818239fe1ce23b9b8973879
sha512: e0ba4a36edb495484beec9d6f0a5ab81655abebed150e3b25c145732b4a13c52fd86da29a31c898b2b3410ba338b31d627b83decfa8a08dc092334ac27b2827d
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a600d91b88e59eb838a4f8320ca72b5db618b8ad1012c9373754e469a8e1caa1
```

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

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

FILE	DETAILS

<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>r8</td></tr></table></td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	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
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	b/b/a/a/f/a.java b/b/a/a/c/c.java b/b/a/a/c/b.java b/b/a/a/c/d.java b/b/a/a/d/c.java b/b/a/a/d/b.java b/b/a/a/d/d.java
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	a/a/c/c/i/e.java a/a/c/c/h.java a/a/d/b/a/b.java a/a/c/c/b.java a/a/c/a/e.java me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java a/a/c/h/c.java a/a/c/a/f.java a/a/c/h/q.java a/a/c/c/e.java butterknife/ButterKnife.java a/a/c/c/i/a.java a/a/d/e/d.java a/a/c/c/f.java com/afollestad/materialdialogs/internal/c.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java a/a/c/h/f.java a/a/c/b/b/b.java a/a/b/a/i.java a/a/c/h/p.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 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
android.googlesource.com	ok	**IP:** 142.250.27.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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.