ANDROID STATIC ANALYSIS REPORT

Titan Companion (v67-beta)

File Name:	installer3821.apk
Package Name:	pt.joaomneto.titancompanion
Scan Date:	May 31, 2022, 7:27 p.m.
App Security Score:	**64/100 (LOW RISK)**
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	4	1	1	2

FILE INFORMATION

File Name: installer3821.apk
Size: 11.89MB
MD5: 3b914a2bc09bd1553d2716515e515eed
SHA1: 435363cb16d07cfe4e2ed76c9a8ec24ceec53879
SHA256: 83c464057199431b15ea70d327a75fa79d8184abeecd28c00125d4bf5e639c2a

APP INFORMATION

App Name: Titan Companion
Package Name: pt.joaomneto.titancompanion
Main Activity: pt.joaomneto.titancompanion.MainActivity
Target SDK: 29
Min SDK: 19
Max SDK:
Android Version Name: v67-beta
Android Version Code: 67

APP COMPONENTS

Activities: 94

Services: 0

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: C=PT, L=Lisboa, OU=joaomneto, CN=Joao Neto
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-03-13 23:09:49+00:00
Valid To: 2042-03-07 23:09:49+00:00
Issuer: C=PT, L=Lisboa, OU=joaomneto, CN=Joao Neto
Serial Number: 0x2208534a
Hash Algorithm: sha256
md5: 99ff57b71b83d3e5c02959e3a78cc6c9
sha1: feb60b779ea15f3539db2212308b80cba1f4e061
sha256: d2ea2143acce59117567ef66ae67bc00d1feb4b78208b31ad4184c35fdc28226
sha512: 7f994ce57e94c00cb7b9b4257d545b1e4fcbb5175ccc5b7531e80fd4a3c891f7c671b7278d57a16d41341ef9f31d5746b3269549a66e81ffcdc128e6fa91f3e5
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: efd878bb88f5a8e519984fec9dba823326f2fdaa6fe31e7292f1ea4ef37e08f0
```

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 PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

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	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 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	pt/joaomneto/titancompanion/adventure/impl/fragments/st/STCombatFragment.java pt/joaomneto/titancompanion/util/DiceRoller.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	pt/joaomneto/titancompanion/MainActivity.java pt/joaomneto/titancompanion/adapter/SavegameListAdapter.java
3	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	pt/joaomneto/titancompanion/TCPreferenceActivity.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 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.
10	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
fightingfantasy.wikia.com	ok	**IP:** 151.101.64.194 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 142.251.36.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

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.