ANDROID STATIC ANALYSIS REPORT

LifeCounter (2.0)

File Name:	installer3824.apk
Package Name:	com.marceljurtz.lifecounter
Scan Date:	May 31, 2022, 7:44 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
1	3	1	1	0

FILE INFORMATION

File Name: installer3824.apk
Size: 3.39MB
MD5: 4918edfd044015ef53032b980e22e446
SHA1: 844a1dc6ec65602eaf213eb04899193fd5f1eddf
SHA256: 1bccbbd1a73f00037debb12a594e0e4512025f222a6d40bb323bf3f8936d6108

APP INFORMATION

App Name: LifeCounter
Package Name: com.marceljurtz.lifecounter
Main Activity: com.marceljurtz.lifecounter.views.Game.GameActivity
Target SDK: 28
Min SDK: 17
Max SDK:
Android Version Name: 2.0
Android Version Code: 15

APP COMPONENTS

Activities: 6
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: 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: 2017-07-19 20:16:53+00:00
Valid To: 2044-12-04 20:16:53+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x306c4289
Hash Algorithm: sha256
md5: b6b95d8f00d556f70b8e91910acb9aaa
sha1: 07b31bb148fe1ae75811526b7d5c5b7c5461ee31
sha256: 72cb5f646408c49c0dec07b0c97a8df82b604ed8bf147dc55a5ea10abb0576ed
sha512: e09132c76ef721b4eebc4abc58a86aa15287af2839343860a835808ac9511108ac4b43b4f81448d99f54d0dc8720167fc58b3b70487daa66c872f77ed60a4117

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.

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>r8 without marker (suspicious)</td></tr></table></td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

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
1	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	com/github/paolorotolo/appintro/AppIntroBase.java
2	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	com/marceljurtz/lifecounter/views/Dicing/DicingPresenter.java com/marceljurtz/lifecounter/views/Counter/CounterPresenter.java com/marceljurtz/lifecounter/models/Dice.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 no hardware resources.
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 no 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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
instagram.com	ok	**IP:** 157.240.201.174 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
youtube.com	ok	**IP:** 142.250.179.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
m.facebook.com	ok	**IP:** 157.240.201.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
paolorotolo.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

✉ EMAILS

EMAIL	FILE
feedback@mjurtz.com	com/marceljurtz/lifecounter/models/AppDetails.java
feedback@mjurtz.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"library_appintro_authorWebsite" : "http://paolorotolo.github.io/"
"library_appintro_authorWebsite" : "http://paolorotolo.github.io/"

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.