MOBSF

ANDROID STATIC ANALYSIS REPORT

Randomix (1.11)

File Name:	installer251.apk
Package Name:	com.minar.randomix
Scan Date:	May 31, 2022, 10:56 a.m.
App Security Score:	67/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	3	1	1	0

FILE INFORMATION

File Name: installer251.apk
Size: 3.22MB
MD5: 20860d984e220714dbbd92371abd2d7e
SHA1: 8b943fe6ef77d79c43523e028ea4a7ddc52c3aad
SHA256: 6e755b9703c3be9fc198cde3ff54d2538c6710492e83d68dfd99d2a068a2883c

APP INFORMATION

App Name: Randomix
Package Name: com.minar.randomix
Main Activity: com.minar.randomix.activities.MainActivity
Target SDK: 30
Min SDK: 24
Max SDK:
Android Version Name: 1.11
Android Version Code: 27

APP COMPONENTS

Activities: 2
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: True
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-08 06:13:40+00:00
Valid To: 2048-03-26 06:13:40+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0xf2bce0e7c7162691
Hash Algorithm: sha256
md5: 7f34b152f701f707590394a16131886a
sha1: e32ed820a0f8fa0de2cde9c4eecb42a55222d7d1
sha256: a77af37eb1fc21b6baca14e8c526dfa9c6e26600f93a3f63c4366b52d0ceda13
sha512: 0fe23751175e4b670a6b3e4935c8e955c2b67bb21151a771a9e03e95af7c15b7586cda10771dcc5a9a3ac62d2c3ace2561732967b8bd8c3a93f99eb1993b3a4e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 36fdd4d5df069fe9edd8ceb0dfc4089c167af6646dfc3c1854c2eef779858ce1
```

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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></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 OWASP MASVS: MSTG-STORAGE-3	a/n/i0.java a/g/e/g.java a/g/j/b.java b/a/a/a/z/d.java a/g/h/b.java a/o/a/a/h.java a/g/e/k.java a/e/b/d.java a/p/a/b.java a/n/y.java a/g/l/b0.java b/a/a/a/c0/g.java b/a/a/a/a0/b.java a/g/d/c/b.java a/i/b/c.java b/a/a/a/p/a.java b/a/a/a/m/h.java a/g/l/u.java a/g/l/t.java a/a/o/g.java a/g/e/f.java a/g/e/c.java com/github/appintro/internal/LogHelper.java a/g/l/b.java a/g/l/c0/c.java a/g/e/j.java a/g/d/c/f.java a/g/k/b.java a/a/k/a/a.java a/g/d/c/a.java a/g/l/h.java a/g/l/w.java a/e/b/k/f.java a/g/e/e.java a/l/a/b.java a/g/l/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/minar/randomix/fragments/RouletteFragment.java com/minar/randomix/fragments/DiceFragment.java com/minar/randomix/fragments/CoinFragment.java com/minar/randomix/fragments/MagicBallFragment.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 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.paypal.me	ok	**IP:** 151.101.129.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.instagram.com	ok	**IP:** 157.240.201.174 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
forum.xda-developers.com	ok	**IP:** 104.18.18.88 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
minar.ml	ok	**IP:** 151.101.1.195 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

✉ EMAILS

EMAIL	FILE
minar.tastic@gmail.com	Android String Resource

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.