

#### ANDROID STATIC ANALYSIS REPORT



PianOli (1.7)

File Name:	installer10.apk
Package Name:	com.nicobrailo.pianoli
Scan Date:	May 30, 2022, 4:23 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

#### FINDINGS SEVERITY

<b>兼</b> HIGH	▲ MEDIUM	<b>i</b> INFO	<b>✓</b> SECURE	≪ HOTSPOT
1	2	1	1	0

#### FILE INFORMATION

File Name: installer10.apk

Size: 1.97MB

MD5: d5f3db97d719ba77528be1d7c008a6f1

**SHA1**: 7e439aa95d9a1eee572d938683973f04d48c76fc

SHA256: d206983ae8638255df695d8298b8ec54720bc7bb4631d9715b1aec2bfafeddaf

#### **i** APP INFORMATION

App Name: PianOli

Package Name: com.nicobrailo.pianoli

Main Activity: com.nicobrailo.pianoli.MainActivity

Target SDK: 28 Min SDK: 21 Max SDK:

Android Version Name: 1.7
Android Version Code: 7

#### **APP COMPONENTS**

Activities: 1 Services: 0 Receivers: 0 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O

#### **\*** 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: 2018-09-10 18:57:40+00:00 Valid To: 2046-01-26 18:57:40+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x700c256f Hash Algorithm: sha256

md5: 4b7c8a7f00c176ea413fd38d1cac8f31

sha1: c8e552de28618f87ba938ca17d33fc04aea8f65f

sha256: f670c9407cbe7cee3e26ed29cbb82a700c49e993759498b6eb97c1f277feb5d9

sha512: fdf2485105b275fadf9db7e58afed0a31f994ad59bd779fb72b1cce41e88bed600d41712feaefe55efa374b87edacee3782b1b1d416902cd40528f06b9cfdc3c

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.

# **M** APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
	Compiler	r8 without marker (suspicious)	

### **△** NETWORK SECURITY

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

## **Q** 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 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/nicobrailo/pianoli/AppConfigTrigg er.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	com/nicobrailo/pianoli/AppConfigTrigg er.java com/nicobrailo/pianoli/MainActivity.jav a com/nicobrailo/pianoli/PianoCanvas.ja va com/nicobrailo/pianoli/Piano.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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.

# **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
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

#### 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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.