

ANDROID STATIC ANALYSIS REPORT



Simple Chess Clock (2.1.1)

File Name:	installer263.apk
Package Name:	com.chessclock.android
Scan Date:	May 31, 2022, 10:10 a.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
2	1	1	1	0

FILE INFORMATION

File Name: installer263.apk

Size: 0.1MB

MD5: 5e063dddc2f320617711fbdccdd2ca4a

SHA1: 2f988dc93e12b4393cfd75b64a8c1b88613e3168

SHA256: 113b6fee9d2138ea0323f21c851bc85c1f67b092b62cb76667a9e627b977f2cd

i APP INFORMATION

App Name: Simple Chess Clock

Package Name: com.chessclock.android

Main Activity: .ChessClock

Target SDK: 23 Min SDK: 21 Max SDK:

Android Version Name: 2.1.1 Android Version Code: 11

B APP COMPONENTS

Activities: 2 Services: 0 Receivers: 0 Providers: 0

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



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: 2012-01-08 15:19:56+00:00 Valid To: 2039-05-26 15:19:56+00:00

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

Serial Number: 0x4f09b41c Hash Algorithm: sha1

md5: c14ceb553533286970aa9a80f3d9515c

sha1: c0241c3e0a664bea75aad98d9091694aad68a01b

sha256: b5d42fd5df73fb73df6afd4271124abe33913cceafc34882616ccd9d8cd60306

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.	
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.	

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

M APKID ANALYSIS

FILE	DETAILS		
classes dev	FINDINGS	DETAILS	
classes.dex	Compiler	dx	



NO	SCOPE	SEVERITY	DESCRIPTION

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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/chessclock/android/ChessClock. java com/chessclock/android/Prefs.java

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	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
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to no hardware resources.
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
7	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.
8	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.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

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
www.gnu.org	ok	IP: 209.51.188.116 Country: United States of America Region: Massachusetts City: Boston Latitude: 42.358429 Longitude: -71.059769 View: Google Map
www.apache.org	ok	IP: 151.101.2.132 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.