

ANDROID STATIC ANALYSIS REPORT



Anuto TD (0.6-1)

File Name:	installer376.apk
Package Name:	ch.logixisland.anuto
Scan Date:	May 31, 2022, 8:04 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

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

FILE INFORMATION

File Name: installer376.apk

Size: 5.99MB

MD5: 3d5d3d542fdecb4250419c8e1a20e3a4

SHA1: 56e696942c6b62932a1fce43b27dc7d6d60e2478

SHA256: d832d534b115a72e145e5fa43c4764ed8738670a32759ee8f48282c8cf624a3d

i APP INFORMATION

App Name: Anuto TD

Package Name: ch.logixisland.anuto

Main Activity: ch.logixisland.anuto.view.game.GameActivity

Target SDK: 30 Min SDK: 17 Max SDK:

Android Version Name: 0.6-1
Android Version Code: 23

EE APP COMPONENTS

Activities: 6 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: 2016-07-03 15:16:43+00:00 Valid To: 2043-11-19 15:16:43+00:00

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

Serial Number: 0x256e59fb Hash Algorithm: sha256

md5: 241cc1cdb07526284e3d875b359e3a1c

sha1: 6eb96ca99545cf9d4327454cdce713c6b45a1cd1

sha256: 65197484d51b46703badc7ca3e45b3b3232fbfb483a6f5a20b5eff4e0583d5a5

sha512: 5ff4abae123a8ca4102e02224cace9caee4cb65ae6942c0751a9b7b6af2fc297fe317bce276ea7283d80eb66e66490484e9a40e88704dea1e4c1bc0edfbea3c2

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	
Clusses.ucx	Compiler	r8	

△ NETWORK SECURITY

NO	SCOPE	CEVEDITY	DESCRIPTION
NO	SCOPE	SEVERITY	DESCRIPTION

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

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 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	ch/logixisland/anuto/util/iterator/StreamIterato r.java ch/logixisland/anuto/util/RandomUtils.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	ch/logixisland/anuto/business/game/GameSav er.java ch/logixisland/anuto/business/game/SaveGam eRepository.java ch/logixisland/anuto/business/game/GameLoa der.java ch/logixisland/anuto/engine/logic/loop/GameL oop.java ch/logixisland/anuto/engine/logic/loop/FrameR ateLogger.java ch/logixisland/anuto/business/wave/WaveMan ager.java

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.
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.

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.