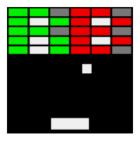


## ANDROID STATIC ANALYSIS REPORT



Retro Breaker (1.3)

File Name:	installer3771.apk
Package Name:	br.usp.ime.retrobreaker
Scan Date:	May 31, 2022, 7:17 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	

### FINDINGS SEVERITY

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

#### FILE INFORMATION

File Name: installer3771.apk

Size: 0.13MB

MD5: 682ff0c4422837e4a4a49f6d1b651333

SHA1: 01901f4f399c0f204f4538a11e6e7808328244f0

SHA256: 9360bdac910fa6800cc92289a37da4f3e793a7e4151c99f9cbf6cf8e6d1e50fc

### **i** APP INFORMATION

App Name: Retro Breaker

Package Name: br.usp.ime.retrobreaker

Main Activity: br.usp.ime.retrobreaker.MainActivity

Target SDK: 28 Min SDK: 14 Max SDK:

Android Version Name: 1.3 Android Version Code: 7

#### **APP COMPONENTS**

Activities: 2 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: 2014-05-27 12:07:20+00:00 Valid To: 2041-10-12 12:07:20+00:00

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

Serial Number: 0x617aaff7 Hash Algorithm: sha256

md5: e0dbd57d4c611b606953eee1a6bf43e6

sha1: a51ad3fd44e7b0bb58858678f3c51faae50351a7

sha256: 50140af5fc8000ad96cbe871694a9c368a30fcce267a882ccbc2bdb0a6543ae1

sha512: c1e0eca36fa74576f316ed37c4e638748c6495c07f5029fb5710d986062846d58d6dfeff389fd9831fcd3402ee24f6192bf68471a9e2e9b910fc5522afbffcd6

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	dx	

## **△** 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 logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	br/usp/ime/retrobreaker/MainActivity .java br/usp/ime/retrobreaker/game/b.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.
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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
www.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

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.