ANDROID STATIC ANALYSIS REPORT

Retro Breaker (1.3)

File Name:	installer3791.apk
Package Name:	br.usp.ime.retrobreaker
Scan Date:	May 31, 2022, 5:55 p.m.
App Security Score:	73/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
0	2	1	1	0

FILE INFORMATION

File Name: installer3791.apk
Size: 0.14MB
MD5: 472c52fe1fbab114b9321334ad126712
SHA1: 472fce27e3868f0e7558f9789da99b8a0a1faf0c
SHA256: 6fa24088fe51f273e4ed709f9e760d25adebd0beafb373aaa2986e945b68e17f

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: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=BR, ST=São Paulo, L=Guarulhos, CN=Thiago Kenji Okada
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-04-30 12:33:48+00:00
Valid To: 2039-04-24 12:33:48+00:00
Issuer: C=BR, ST=São Paulo, L=Guarulhos, CN=Thiago Kenji Okada
Serial Number: 0x1befdc0a
Hash Algorithm: sha256
md5: 3d4da866ac35665e69ee1c10befbf051
sha1: f1b53450dedefb0e048334b8a85ca6f47e15ae30
sha256: e30a5f32969fec8e49a2997000505bb0f337d1c103b695969d01e6b01b3f6661
sha512: ded6ed6a8941075a3dd735c4f1eeccff77be82f75620b660f679952b65a23367c59ce205a67dca673dea3c0c4ca54f2262559401c220e1a2e34019808fd8af12
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8b489c76d4015d5d28887eb4849ff4df1982f32b4418c2e63e47f72d21296b83
```

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.

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>Compiler</td><td>dx</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
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/game/b.java br/usp/ime/retrobreaker/MainActivity.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.

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.