

ANDROID STATIC ANALYSIS REPORT



• Memo Game (1.0.2)

File Name:	installer3822.apk
Package Name:	org.secuso.privacyfriendlymemory
Scan Date:	May 31, 2022, 7:14 p.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: installer3822.apk

Size: 4.71MB

MD5: 5614abc7ba02aeeed7e85a65e1dd6260

SHA1: 7f4b097f6e65930823272544ce4ad98e02a75a17

SHA256: 002300512f2fc3e40b3bda6507f0fa90cd46a5ed22bf806bd2f4d0bd314416dc

i APP INFORMATION

App Name: Memo Game

 $\label{package Name: proposed proposed package Name: or g. secuso. privacy friendly memory$

Main Activity: org.secuso.privacyfriendlymemory.ui.SplashActivity

Target SDK: 25 Min SDK: 17 Max SDK:

Android Version Name: 1.0.2 Android Version Code: 3

EE APP COMPONENTS

Activities: 8 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: 2016-11-26 17:16:17+00:00 Valid To: 2044-04-13 17:16:17+00:00

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

Serial Number: 0x619d9b05 Hash Algorithm: sha256

md5: 34521f37c7ec88491a86462910f411cd

sha1: 57af8de436b9f2f20ae4b3f8783395490d9f86cd

sha256: 9dd96e14306c971f999f05e00599c8c9c17f83657972875bd22678dd937438bd

sha512: 1cd1d46827c088eeda9ed775a201fae09beba696e4ddc90ae6a13d40679f9db33f9784b20ccd6c313061a88fa865ae4df6c9472017a5274ad05cf657dd3795d3

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		
	FINDINGS	DETAILS	
classes.dex	Compiler	dx (possible dexmerge)	
	Manipulator Found	dexmerge	

△ NETWORK SECURITY

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

Q 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	org/secuso/privacyfriendlymemory/ui/navigation/ DeckChoiceActivity.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 implement functionality to encrypt sensitive data 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 encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

▶ HARDCODED SECRETS



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.