

ANDROID STATIC ANALYSIS REPORT



Number Guesser (4.2.0)

taller289.apk
m.numguesser.tonio_rpchp.numberguesser
y 31, 2022, 9:47 a.m.
5/100 (MEDIUM RISK)
1

FINDINGS SEVERITY

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

FILE INFORMATION

File Name: installer289.apk

Size: 1.6MB

MD5: 3103ccb95633828183979f8350efc924

SHA1: f6ff0b1e08e02383a889390bbe77af7faf3f8a1c

SHA256: 442c1956932b442e4e5756ca9f00fff7a615ade094d84c04605c2e0899ae4603

i APP INFORMATION

App Name: Number Guesser

Package Name: com.numguesser.tonio_rpchp.numberguesser

 ${\it Main\ Activity:} com.numguesser.tonio_rpchp.numberguesser.Guesser$

Target SDK: 28 Min SDK: 14 Max SDK:

Android Version Name: 4.2.0 Android Version Code: 13

APP COMPONENTS

Activities: 1 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: 2014-11-30 06:51:19+00:00 Valid To: 2042-04-17 06:51:19+00:00

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

Serial Number: 0x9a7fd16 Hash Algorithm: sha256

md5: 284ce29cb778abe69d0915d04f7b1034

sha1: 2731ea18789bd4231af2de4c4886263fd875ab8a

sha256: 6121659eca7319db33f67adb759f5c229889ec19081dcfce86642dbfd1597377

sha512: ce8e90ceb2e736f61439a86f1946ad5f2a71cbd2b5caca3f09300b95771d3ca94551e018cfdd7de3b4a63408b5b81b841d8af6f0d84b4f8d6ac88bf984189c2a

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.

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

MAPKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
classes.uex	Compiler	r8	

△ NETWORK SECURITY

	1	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 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	com/numguesser/tonio_rpchp/numberguesser/Gu esser.java

■ NIAP ANALYSIS v1.3

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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 implement functionality to encrypt sensitive data 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 encrypt some transmitted data with HTTPS/TLS/SSH 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.