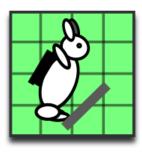


### ANDROID STATIC ANALYSIS REPORT



Rabbit Escape (0.13)

File Name:	installer3854.apk
Package Name:	net.artificialworlds.rabbitescape
Scan Date:	May 31, 2022, 6:47 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

#### FINDINGS SEVERITY

<b>派</b> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	≪ HOTSPOT
1	2	1	1	0

#### FILE INFORMATION

File Name: installer3854.apk

Size: 18.37MB

MD5: d3eb2c78567e165ae15b26de653498f0

**SHA1**: f4e0f83e1ecffc7fc658a456f4c5327ad170b657

SHA256: bf8d0dc3018d773710a6fe626973d93230f65415d7a11010c2b16267ab5e7568

#### **i** APP INFORMATION

App Name: Rabbit Escape

Package Name: net.artificialworlds.rabbitescape

Main Activity: rabbitescape.ui.android.AndroidMenuActivity

Target SDK: 26 Min SDK: 14 Max SDK:

Android Version Name: 0.13
Android Version Code: 130

#### **APP COMPONENTS**

Activities: 3 Services: 0 Receivers: 0 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O



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: 2017-01-30 13:52:34+00:00 Valid To: 2044-06-17 13:52:34+00:00

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

Serial Number: 0x6c3dde71 Hash Algorithm: sha256

md5: 39626203e0dfb3e1713eb520b0321a1b sha1: d59e1741c19cfe8bf7afbc477a07e7fdd9a9503e

sha256: d0d66c2dff3ea616c081360588acf2a31989db4148e8e4281370c6acd76a79cb

sha512: 7f2162e9dab1cbf8053c9a45cb00b7be94e69b3e43e161561679b1ec8ab4966b68cda026f8b43cf2b3220dc02fb2caa1a1de2d8b6a11363abb5a479354b70d7b

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	r8	

## **△** 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 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	rabbitescape/render/WaterParticle.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	rabbitescape/ui/android/AndroidGraphi cs.java rabbitescape/engine/config/TapTimer.ja va

# ■ 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.

# **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
www.artificialworlds.net	ok	IP: 75.119.215.162 Country: United States of America Region: California City: Brea Latitude: 33.930222 Longitude: -117.888420 View: Google Map
tryad.org	ok	IP: 143.95.72.227 Country: United States of America Region: Massachusetts City: Burlington Latitude: 42.508480 Longitude: -71.201134 View: Google Map

#### 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.