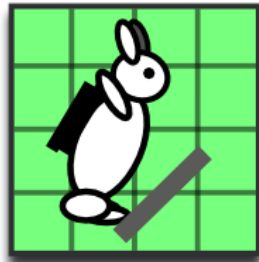




ANDROID STATIC ANALYSIS REPORT



 Rabbit Escape (0.11)

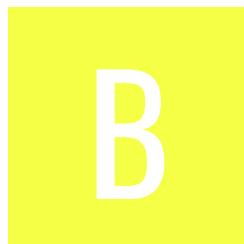
File Name: `installer3843.apk`

Package Name: `net.artificialworlds.rabbitescape`






Scan Date: May 31, 2022, 6:52 p.m.

App Security Score: **55/100 (MEDIUM RISK)**

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	2	1	1	0

FILE INFORMATION

File Name: installer3843.apk

Size: 20.19MB

MD5: 48f9699b6df36622db32a620cb7dd6fa

SHA1: 58b3d14da5c3b8147917929005da768c0f16ceab

SHA256: b075a29c95f1422e69417495f56ca1c84be19dd124ef57b3f8137778ace0f0cc

APP INFORMATION

App Name: Rabbit Escape

Package Name: net.artificialworlds.rabbitescape

Main Activity: rabbitescape.ui.android.AndroidMenuActivity

Target SDK: 21

Min SDK: 8

Max SDK:

Android Version Name: 0.11

Android Version Code: 110

APP COMPONENTS

Activities: 3

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: 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.



APKID ANALYSIS

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



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	rabbitescape/engine/util/WorldAssertio ns.java rabbitescape/engine/config/TapTimer.ja va rabbitescape/render/TestAnimations.jav a rabbitescape/render/SpriteAnimator.jav a rabbitescape/ui/android/AndroidGraphi cs.java rabbitescape/engine/WaterRegionFactor y.java rabbitescape/engine/WaterRegion.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	rabbitescape/render/AnimationLoader.j ava

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.
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.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
rabbit.com	ok	IP: 66.77.174.59 Country: United States of America Region: Minnesota City: Plymouth Latitude: 45.010521 Longitude: -93.455513 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
example.com	ok	IP: 93.184.216.34 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 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](#).