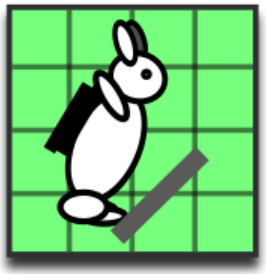
MOBSF

ANDROID STATIC ANALYSIS REPORT



Rabbit Escape (0.13)

File Name:	installer3829.apk
Package Name:	net.artificialworlds.rabbitescape
Scan Date:	May 31, 2022, 5:56 p.m.
App Security Score:	67/100 (LOW RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	3	1	1	0

FILE INFORMATION

File Name: installer3829.apk
Size: 18.24MB
MD5: e8e95960dd75a9b489371ba7695d5763
SHA1: a94d6333bb92f9ea96ce933c5b45de228aafc8b5
SHA256: 3c1e5aa926673cade29e0e6aa9aa5a5a5719c0c23761ca0247ea946459e01af8

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: 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=UK, O=Rabbit Escape, CN=Andy Balaam
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-03-05 03:58:41+00:00
Valid To: 2040-02-27 03:58:41+00:00
Issuer: C=UK, O=Rabbit Escape, CN=Andy Balaam
Serial Number: 0x508d7158
Hash Algorithm: sha256
md5: 06504b511c500ab537153d5cda01ff3d
sha1: 611433697deee083a3940860af8e9a8e696a98b0
sha256: 55e372eedf58f5482e5e9870c9c711b4cd5be7293914ef3882817c38b855faf2
sha512: aa4634ac99c63630b17811cbf954f6d27c48dbd69790b232432dbd60a2be51477cc711ddc7bce751bf9e94d68a29677304259f884e6084ee47db17ee94859bcb
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: dab8a192c8f23e2b03892e44700e8dddb78845ab3e61e7b77eb74448eab14632

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

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: r8

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/ui/android/AndroidGraphics.java rabbitescape/engine/config/TapTimer.java
2	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

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.

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.