MOBSF

ANDROID STATIC ANALYSIS REPORT

Enchanted Fortress (1.14)

File Name:	installer52.apk
Package Name:	hr.kravarscan.enchantedfortress
Scan Date:	May 31, 2022, 12:04 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	2	1	1	0

FILE INFORMATION

File Name: installer52.apk
Size: 1.15MB
MD5: 4d40f2f35b5b98865f056e560d9d7eef
SHA1: 74239ca4b773dcc5ad8e4eb933c6e5678c850091
SHA256: 4571d4fce7864727ea2a31b50235ca1e1208b8ac66c5148f825abae4ccf66b0d

APP INFORMATION

App Name: Enchanted Fortress
Package Name: hr.kravarscan.enchantedfortress
Main Activity: hr.kravarscan.enchantedfortress.MainActivity
Target SDK: 28
Min SDK: 15
Max SDK:
Android Version Name: 1.14
Android Version Code: 15

APP COMPONENTS

Activities: 8
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: 2017-05-29 10:40:53+00:00
Valid To: 2044-10-14 10:40:53+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x30926910
Hash Algorithm: sha256
md5: 2c15bab13d20c4e5a847463c828fe4cd
sha1: 57e0a173bdd3fb36183aa148217d2e74efd4fee4
sha256: 70b091183000cdea42a8c9359be926457399e22dad87a0c47fd77cfa96d4e36f
sha512: b30330c855ca4d0392bcf3e10957bcc64af93007bcfb872e35af164bad94d91bba677ad729de9e5377ab6d16d9c0f7942990faca43a8f9119c86900bb129c971

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: Compiler — DETAILS: unknown (please file detection issue!)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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 logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	hr/kravarscan/enchantedfortress/ScoresActivity.java a/d/k/b.java a/d/d/c/f.java hr/kravarscan/enchantedfortress/HelpActivity.java a/d/k/c0/c.java a/d/d/c/b.java hr/kravarscan/enchantedfortress/b/d.java a/d/d/c/a.java hr/kravarscan/enchantedfortress/AboutActivity.java a/d/e/h.java a/d/e/i.java hr/kravarscan/enchantedfortress/a/c.java hr/kravarscan/enchantedfortress/b/a.java a/d/e/e.java a/d/e/f.java hr/kravarscan/enchantedfortress/GameActivity.java a/a/k/a/a.java hr/kravarscan/enchantedfortress/MainActivity.java hr/kravarscan/enchantedfortress/a/b.java a/d/k/w.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/d/e/b.java hr/kravarscan/enchantedfortress/NewsActivity.java a/h/a/b.java a/d/e/d.java a/d/k/g.java a/d/k/u.java hr/kravarscan/enchantedfortress/SettingsActivity.java hr/kravarscan/enchantedfortress/a/a.java a/d/k/t.java hr/kravarscan/enchantedfortress/NewGameActivity.java a/j/a/a/i.java a/d/k/e.java a/d/j/b.java a/a/o/g.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	hr/kravarscan/enchantedfortress/a/b.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 does not encrypt files 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
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.paypal.me	ok	**IP:** 23.32.9.126 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **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.