MOBSF

ANDROID STATIC ANALYSIS REPORT

Enchanted Fortress (1.15)

File Name:	installer357.apk
Package Name:	hr.kravarscan.enchantedfortress
Scan Date:	May 31, 2022, 4:42 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: installer357.apk
Size: 1.13MB
MD5: d7d69404babe1230a6068258076ed345
SHA1: 545dde5120ed6dfcdb55dd6ef609f6b1244edde6
SHA256: bfb8512e0af1da7d7ce5a9d4aef6c82c0340a93383f2d07199382b89ebe97744

APP INFORMATION

App Name: Enchanted Fortress
Package Name: hr.kravarscan.enchantedfortress
Main Activity: hr.kravarscan.enchantedfortress.MainActivity
Target SDK: 30
Min SDK: 15
Max SDK:
Android Version Name: 1.15
Android Version Code: 16

APP COMPONENTS

Activities: 8
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Missing certificate
v1 signature: False
v2 signature: False
v3 signature: False

TITLE	SEVERITY	DESCRIPTION
Missing Code Signing certificate	high	Code signing certificate not found

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

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	a/i/a/b.java hr/kravarscan/enchantedfortress/a/b.java hr/kravarscan/enchantedfortress/b/b.java hr/kravarscan/enchantedfortress/b/a.java a/d/e/i.java a/a/k/a/a.java a/d/d/c/f.java a/d/k/s.java a/d/e/d.java a/d/k/u.java a/d/k/e.java hr/kravarscan/enchantedfortress/HelpActivity.java a/d/j/b.java a/d/d/c/b.java a/d/d/c/a.java a/d/k/r.java a/d/k/a0/c.java hr/kravarscan/enchantedfortress/AboutActivity.java a/d/e/b.java hr/kravarscan/enchantedfortress/GameActivity.java a/d/k/g.java a/d/k/b.java a/a/o/g.java hr/kravarscan/enchantedfortress/NewsActivity.java hr/kravarscan/enchantedfortress/a/c.java a/d/e/h.java hr/kravarscan/enchantedfortress/MainActivity.java hr/kravarscan/enchantedfortress/ScoresActivity.java hr/kravarscan/enchantedfortress/a/d.java hr/kravarscan/enchantedfortress/b/f.java hr/kravarscan/enchantedfortress/SettingsAct

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ivity.java a/d/e/e.java hr/kravarscan/enchantedfortress/NewGame
				Activity.java a/d/e/f.java a/k/a/a/h.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/a.java hr/kravarscan/enchantedfortress/a/c.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.
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.paypal.me	ok	**IP:** 151.101.65.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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.