ANDROID STATIC ANALYSIS REPORT

app_icon

Find my secret (1.0)

File Name:	app-docker.apk
Package Name:	com.ecw2022.findmysecret
Scan Date:	Nov. 3, 2022, 10:15 a.m.
App Security Score:	85/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	i INFO	✓ SECURE	HOTSPOT
0	1	1	1	0

FILE INFORMATION

File Name: app-docker.apk
Size: 8.75MB
MD5: 2bda537341fbbf18c9f73da27891f2ae
SHA1: 9265391663782a38100416ae54b952164ae7d9d4
SHA256: 8d3f262f9525251b13d4aec9b3fd0c8bb9a5ecb2b650010705883 91fa7ba7817

APP INFORMATION

App Name: Find my secret
Package Name: com.ecw2022.findmysecret
Main Activity: com.ecw2022.findmysecret.MainActivity
Target SDK: 32
Min SDK: 31
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 1
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: False
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=FR, OU=ECW
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-08-16 11:35:01+00:00
Valid To: 2047-08-10 11:35:01+00:00
Issuer: C=FR, OU=ECW
Serial Number: 0xfa50b1a
Hash Algorithm: sha256
md5: 8706c78464ed4e0b4f68faf75a222d6a
sha1: 31d5719008f7a18fa00ad8e2e607a14e0a1091c6
sha256: 9ce456c89021f1584db91424f760fbe176bf580fad01d827c498335563f1cc38
sha512: 88d4575a22ac54ec0ba0c6c83c459094f29b7764196493e80a67979a5031002f7f5ac84c36511f565b22faeb110348908b2b5c38e19a9043e3d83b905a075db8
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: fe8058183bd9be8d9034f14f91ae10b94323ad79aaa20927427390ddc2b37bf3
```

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

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	com/ecw2022/findmysecret/MainActivity.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.

Report Generated by - MobSF v3.6.1 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.