ANDROID STATIC ANALYSIS REPORT

app_icon

DogsApi (1.0)

File Name:	app-release.apk
Package Name:	com.put.dogapi
Scan Date:	Nov. 25, 2022, 7:39 p.m.
App Security Score:	60/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	6	1	1	1

FILE INFORMATION

File Name: app-release.apk
Size: 18.23MB
MD5: e4c2b23581b989235f417319028d15d5
SHA1: 4f7df5d2025ecac579763635dfd87180261e24f5
SHA256: 87cef1584e8e957613f63d186041f2f4e0e2912efd69735a1eed711b9280c351

APP INFORMATION

App Name: DogsApi
Package Name: com.put.dogapi
Main Activity: com.put.dogapi.MainActivity
Target SDK: 33
Min SDK: 28
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 4
Services: 1
Receivers: 1
Providers: 2
Exported Activities: 2
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: False
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=sad
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-11-25 19:34:25+00:00
Valid To: 2047-11-19 19:34:25+00:00
Issuer: CN=sad
Serial Number: 0x6391f8ba
Hash Algorithm: sha256
md5: de065a24863cea8526b1cd3acda22bdb
sha1: 6b3eea8dbc263b6339751e021d74283ffc861d6d
sha256: d96d57c2d6f74d25864bd9c7310abbba086ca440df2ccc4264b6dcda7f4d4bb9
sha512: 2a69b2d61d084be477418bbbcb2ca6cc741dfd5779c416aa516a62b3f5f08dcdba3227287d093938d955a52d4579004c5a1bfca46f09437fa730df9d05932ad4
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f9bd8b3d48e4ef0d6d7bb3ce011ca6320605c7665e7e783291a3e6f098799235
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.put.dogapi.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

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.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.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>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.
2	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	coil/memory/MemoryCache.java com/put/dogapi/ui/screens/login/LoginState.java com/put/dogapi/ui/screens/register/RegisterState.java
2	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/junit/rules/TemporaryFolder.java
3	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	retrofit2/mock/NetworkBehavior.java
4	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	junit/runner/BaseTestRunner.java junit/runner/Version.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 invoke platform-provided 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 implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
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 user/application initiated 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.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
14	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
15	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
16	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
cdn2.thedogapi.com	ok	**IP:** 172.67.167.130 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.thedogapi.com	ok	**IP:** 142.250.74.51 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"api_url" : "https://api.thedogapi.com/"
"google_api_key" : "AIzaSyCrITJ8qRXJ6Ze1po8BqWM1EBRdJS2JhnI"
"google_crash_reporting_api_key" : "AIzaSyCrITJ8qRXJ6Ze1po8BqWM1EBRdJS2JhnI"
"password" : "Password"

Report Generated by - MobSF v3.6.2 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.