

ANDROID STATIC ANALYSIS REPORT



• Dagger (1.1.2)

Grade:	A
App Security Score:	62/100 (LOW RISK)
Scan Date:	May 31, 2022, 11 a.m.
Package Name:	com.nikola.jakshic.dagger
File Name:	installer292.apk

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	♥ HOTSPOT
1	4	1	2	0

FILE INFORMATION

File Name: installer292.apk

Size: 2.86MB

MD5: 07ff30c83cd152ef755459a0debe8c5c

SHA1: 4b5450a991eded350dccc796a87e788136a083dc

SHA256: 4df96e070c77352c6e6870aed791d5e6849e11c4a09e482a22b58926976e672d

i APP INFORMATION

App Name: Dagger

Package Name: com.nikola.jakshic.dagger

Main Activity: com.nikola.jakshic.dagger.HomeActivity

Target SDK: 29 Min SDK: 16 Max SDK:

Android Version Name: 1.1.2 Android Version Code: 23

EE APP COMPONENTS

Activities: 6 Services: 0 Receivers: 0 Providers: 1

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O



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: 2020-09-08 06:02:37+00:00 Valid To: 2048-01-25 06:02:37+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x36c2fa40 Hash Algorithm: sha256

md5: 4701c24efedf064b1686a9d1eaacdf6a

sha1: ffb37ababd31cccafb5ee131516aa996a56bc2fc

sha256: 5c07c1b066af4897dee2d8ea36f1c74cb746e5f9df7f67341969ace00eaab27a

sha512: 7e1a1095b7d210f4ce92fd195a2b042fc5222f63f71290aa0788f557753009b67ac7ddf255f4fe68bf5cfab5554a85239e6c4fd1bc9bdea729f425865f2a92ac

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.

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

ক্ল APKID ANALYSIS

FILE	DETAILS				
classes.dex	FINDINGS	DETAILS			
	Compiler	unknown (please file detection issue!)			



NO SCOPE SEVERITY DESCRIPTION	Ī	NO	SCOPE	SEVERITY	DESCRIPTION
-------------------------------	---	----	-------	----------	-------------

Q 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
----	-------	----------	-----------	-------

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	d/q/d0.java d/r/a/a/i.java d/a/n/g.java d/i/b/a.java d/j/a/a.java d/g/e/f.java d/g/e/c.java d/g/m/x.java d/g/m/v.java d/g/d/c/b.java d/g/m/b.java d/g/m/b.java d/q/e0.java d/g/e/c.java d/g/e/e.java d/g/m/h.java d/g/e/g.java d/g/m/h.java d/g/e/s.java d/g/e/s.java d/g/m/f.java d/g/m/f.java d/g/m/f.java d/g/k/a.java d/g/k/a.java d/g/k/a.java d/g/k/a.java d/g/k/a.java d/g/m/c0.java d/g/m/c0.java d/g/m/c0.java d/g/m/c0.java d/g/m/c0.java d/g/m/c0.java d/g/m/c0.java d/g/m/c0.java d/g/m/siava d/g/m/siava d/g/m/siava d/g/m/co.java d/g/m/co.java d/g/m/siava d/g/go.java d/q/go.java

NO 2	this Wep uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	SEVERITY secure	STANDARDS OWASP MASVS: MSTG-NETWORK-4	Fight Sava com/nikola/jakshic/dagger/g /s.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	i/z/b.java i/z/d/a.java i/z/a.java
4	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	com/nikola/jakshic/dagger/st ream/i.java e/r/g.java coil/memory/m.java com/nikola/jakshic/dagger/st ream/Stream.java
5	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	d/p/a/f/a.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 ['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 does not encrypt files in non-volatile memory.
8	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.
9	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
10	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.
11	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.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.dota2.com	ok	IP: 104.18.37.57 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map
ns.adobe.com	ok	No Geolocation information available.
dagger-proxy-twitch.herokuapp.com	ok	IP: 3.216.88.24 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
api.opendota.com	ok	IP: 188.114.96.0 Country: Spain Region: Madrid, Comunidad de City: Madrid Latitude: 40.416500 Longitude: -3.702560 View: Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
player.twitch.tv	ok	IP: 199.232.150.167 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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.