

ANDROID STATIC ANALYSIS REPORT



DSA Assistent (Mister English)

File Name:	installer3820.apk
Package Name:	eu.roggstar.luigithehunter.dsaassistent
Scan Date:	May 31, 2022, 7:25 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	

### **FINDINGS SEVERITY**

<b>派</b> HIGH	▲ MEDIUM	<b>i</b> INFO	<b>✓</b> SECURE	♥ HOTSPOT
1	3	1	1	0

#### FILE INFORMATION

File Name: installer3820.apk

Size: 3.1MB

MD5: 2a62c9830f562554ecda00605ad547c7

**SHA1**: 6224c1de4ad064a4b37deccea807def9b6bbe79e

SHA256: a6ad156d4b5d931a59e7e36091f346660bd4d526a05922a79bc46e89921ff39c

## **i** APP INFORMATION

App Name: DSA Assistent

 $\label{package Name: euroggstar.luigithehunter.dsa assistent} \textbf{Package Name: } \textbf{eu.roggstar.luigithehunter.dsa assistent}$ 

Main Activity: eu.roggstar.luigithehunter.dsaassistent.MainActivity

Target SDK: 28 Min SDK: 15 Max SDK:

Android Version Name: Mister English

Android Version Code: 52

#### **EE** APP COMPONENTS

Activities: 7 Services: 0 Receivers: 0 Providers: 0

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

# **\*** 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: 2019-06-06 08:26:01+00:00 Valid To: 2046-10-22 08:26:01+00:00

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

Serial Number: 0x48d00ab0 Hash Algorithm: sha256

md5: ac809c3adbdf61fb672131f965bae30f

sha1: 96b0ef149dd911226e64a8900574f42fa94127b3

sha256: 7a5ad4e2f66bbe99889975cdec8e4c2b5794d8b1d7b4b0221a6fe304c82d8285

sha512: 4776b698d20f87a5c8a3e5b9f6dd76957a61bcd855bc06491b67a10b21584e9855dfd9d2747c9eb4138083d7c98e4fc17bad39cff97f540a390a46ac477ef3ae

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.

# **M** APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
	Compiler	r8	

# **△** NETWORK SECURITY

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

# **Q** 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
				com/bumptech/glide/load/resource/bitmap/Transfo rmationUtils.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/manager/SupportRequestMan agerFragment.java com/bumptech/glide/load/resource/bitmap/Bitmap Encoder.java com/bumptech/glide/load/model/ResourceLoader.j ava com/bumptech/glide/load/resource/bitmap/DefaultI mageHeaderParser.java com/bumptech/glide/load/model/StreamEncoder.ja va com/bumptech/glide/load/model/StreamEncoder.ja va com/bumptech/glide/util/ContentLengthInputStrea m.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/load/engine/executor/GlideEx ecutor.java com/bumptech/glide/load/engine/cache/MemorySiz eCalculator.java com/bumptech/glide/load/resource/gif/ByteBufferG ifDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferG ifDecoder.java com/bumptech/glide/gifdecoder/GifHeaderParser.ja va com/bumptech/glide/gifdecoder/GifHeaderParser.ja va com/bumptech/glide/manager/DefaultConnectivity

NO	ISSUE	SEVERITY	STANDARDS	Monitor.java  Hola Sumptech/glide/load/engine/bitmap_recycle/Lr  uArrayPool.java
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/bumptech/glide/load/resource/bitmap/Hardwa reConfigState.java com/bumptech/glide/load/resource/gif/StreamGifD ecoder.java com/bumptech/glide/gifdecoder/StandardGifDecod er.java com/bumptech/glide/load/resource/bitmap/Downs ampler.java com/bumptech/glide/Glide.java com/bumptech/glide/load/model/ByteBufferEncode r.java com/bumptech/glide/load/model/ByteBufferEncode r.java com/bumptech/glide/load/data/mediastore/Thumb nailStreamOpener.java com/bumptech/glide/load/engine/GlideException.ja va com/bumptech/glide/load/resource/bitmap/VideoD ecoder.java com/bumptech/glide/load/resource/bitmap/VideoD ecoder.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/mediastore/Thumb Fetcher.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/resource/bitmap/Drawab leToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/Drawab leToBitmapConverter.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/executor/Runtime Compat.java com/bumptech/glide/load/engine/executor/Runtime Compat.java com/bumptech/glide/load/engine/bitmap_recycle/Lr uBitmapPool.java

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/signature/ApplicationVersionSi
				MonitorFactory.java com/bumptech/glide/load/engine/prefill/BitmapPre FillRunner.java com/bumptech/glide/load/resource/gif/GifDrawable Encoder.java com/bumptech/glide/load/engine/SourceGenerator. java com/bumptech/glide/load/engine/cache/DiskLruCac heWrapper.java com/bumptech/glide/load/data/AssetPathFetcher.ja va com/bumptech/glide/manager/RequestManagerRetr iever.java com/bumptech/glide/request/target/CustomViewTar get.java
2	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/bumptech/glide/load/engine/DataCacheKey.jav a com/bumptech/glide/load/engine/ResourceCacheKe y.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/EngineResource.j ava com/bumptech/glide/manager/RequestManagerRetr iever.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	eu/roggstar/luigithehunter/dsaassistent/DiceActivity. java



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.
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	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.

#### **Q** DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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
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.

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