MOBSF

ANDROID STATIC ANALYSIS REPORT

DSA Assistent (Mister English)

File Name:	installer3809.apk
Package Name:	eu.roggstar.luigithehunter.dsaassistent
Scan Date:	May 31, 2022, 7:29 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	3	1	1	0

FILE INFORMATION

File Name: installer3809.apk
Size: 3.07MB
MD5: 14ac67b9abaa7a47f22caeab8db85555
SHA1: aef1d5557be4dbf4b3692f688f0ab6dfbb3f80ba
SHA256: 601008a9c1858160ac29405ff1f5b781f8078f396c9a968c828904ddaf11d79f

APP INFORMATION

App Name: DSA Assistent
Package Name: eu.roggstar.luigithehunter.dsaassistent
Main Activity: eu.roggstar.luigithehunter.dsaassistent.MainActivity
Target SDK: 28
Min SDK: 15
Max SDK:
Android Version Name: Mister English
Android Version Code: 55

APP COMPONENTS

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

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=GER, ST=NRW, L=Bad Driburg, CN=Phil Roggenbuck
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-04-14 19:37:26+00:00
Valid To: 2041-04-08 19:37:26+00:00
Issuer: C=GER, ST=NRW, L=Bad Driburg, CN=Phil Roggenbuck
Serial Number: 0x1d09419
Hash Algorithm: sha256
md5: 1f1a868721d5caf8a552a0ce8ed89e95
sha1: e4c77d0354447752793ca8f73b90ba98274c3012
sha256: fba8e0e7fc510e57ced7e6d2d3cc006388337b98531179a5932987a6ec617fee
sha512: ebb30f81dfaf8de3475e9b2e8e7a6625162f7ee16df111bbd02a0d0577142fb543753bc328db14421b6093e3f5e22067637e7bf09480ce900509ba31560580a1

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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Compiler: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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/engine/DecodeJob.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/Glide.java

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/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/util/pool/FactoryPools.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/request/target/CustomViewTarget.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.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	eu/roggstar/luigithehunter/dsaassistent/DiceActivity.java
3	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/Option.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/ResourceCacheKey.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.
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.

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.phrogg.de	ok	**IP:** 188.68.47.208 **Country:** Germany **Region:** Baden-Wurttemberg **City:** Karlsruhe **Latitude:** 49.004719 **Longitude:** 8.385830 **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.