

ANDROID STATIC ANALYSIS REPORT



• Checkers (1.1)

File Name:	installer3799.apk
Package Name:	org.secuso.privacyfriendlydame
Scan Date:	May 31, 2022, 7:33 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	3	1	1	0

FILE INFORMATION

File Name: installer3799.apk

Size: 2.36MB

MD5: 0856c09157b4275aeba77ce9ac7a0b1f

SHA1: bac2318096a442f8bf6fa2695778828c36d56d96

SHA256: cf9af08941dbe19420c22fad6630722eda3db1707d513f16bf83b68fd04e95a4

i APP INFORMATION

App Name: Checkers

Package Name: org.secuso.privacyfriendlydame

 $\textbf{\textit{Main Activity}}: or g. secuso. privacy friendly dame. ui. Splash Activity$

Target SDK: 28 Min SDK: 21 Max SDK:

Android Version Name: 1.1 Android Version Code: 2

EE APP COMPONENTS

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

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: 2018-06-02 05:14:59+00:00 Valid To: 2045-10-18 05:14:59+00:00

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

Serial Number: 0x67d636ec Hash Algorithm: sha256

md5: 7a2c925e091818629fc7f6c4bf3b70ec

sha1: 0bcf594266b359ae3aae98ed3a5518abf86b45d5

sha256: 1475b51d9f05b2723a789676ad07267b74119b4a48bad397cbb140d4fa8e9dcb

sha512: 0c19abaec4433a778c72f5979c684120c07c49e909bef1a4526109d247dab3d60b70aa20946cf4afa5f777e112ccd4002c5e8b72773d530c878e90af5b86afc8

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		
Classes.uex	Compiler	r8	

△ NETWORK SECURITY

NO SCOPE SEVERITY DESCRIPTION

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

١	10	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/gif/ByteBufferG ifDecoder.java com/bumptech/glide/manager/RequestManagerRetr iever.java com/bumptech/glide/load/engine/bitmap_recycle/Lr uArrayPool.java com/bumptech/glide/load/data/mediastore/Thumb nailStreamOpener.java com/bumptech/glide/load/resource/gif/StreamGifD ecoder.java com/bumptech/glide/load/resource/bitmap/Downs ampler.java com/bumptech/glide/load/resource/bitmap/Transfo rmationUtils.java com/bumptech/glide/load/resource/bitmap/Transfo rmationUtils.java com/bumptech/glide/load/resource/bitmap/Defaultl mageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Defaultl mageHeaderParser.java com/bumptech/glide/load/model/FileLoader.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/model/ByteBufferFileLoa

NO	ISSUE	SEVERITY	STANDARDS	der.java der.java der.java ecutor/glide/load/engine/executor/GlideEx
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/manager/DefaultConnectivity Monitor.java com/bumptech/glide/gifdecoder/GifHeaderParser.ja va com/bumptech/glide/load/resource/bitmap/Hardwa reConfigState.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/resource/bitmap/Drawab leToBitmapConverter.java com/bumptech/glide/load/data/mediastore/Thumb Fetcher.java com/bumptech/glide/load/data/mediastore/Thumb Fetcher.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/bitmap_recycle/Lr uBitmapPool.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/prefill/BitmapPre FillRunner.java com/bumptech/glide/load/engine/prefill/BitmapPre FillRunner.java com/bumptech/glide/load/engine/cache/DiskLruCac heWrapper.java com/bumptech/glide/load/engine/SourceGenerator.java

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/manager/RequestManagerFra
				get.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/Glide.java com/bumptech/glide/load/engine/executor/Runtime Compat.java com/bumptech/glide/load/resource/bitmap/Bitmap Encoder.java com/bumptech/glide/manager/DefaultConnectivity MonitorFactory.java com/bumptech/glide/load/model/ByteBufferEncode r.java com/bumptech/glide/load/engine/cache/MemorySiz eCalculator.java com/bumptech/glide/load/resource/gif/GifDrawable Encoder.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/manager/RequestManagerRetr iever.java 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

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	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
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to no hardware resources.
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no network communications.
6	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.
7	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.
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_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.



POSSIBLE SECRETS	
"about_author" : "Authors:"	
"about_author" : "Autoren:"	

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.