ANDROID STATIC ANALYSIS REPORT

🤖 Checkers (1.2)

File Name: installer3830.apk

Package Name: org.secuso.privacyfriendlydame

Scan Date: May 31, 2022, 7:47 p.m.

App Security Score: 54/100 (MEDIUM RISK)

Grade: B

◔ FINDINGS SEVERITY

✿ HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	⚙ HOTSPOT
1	3	1	1	0

⬂ FILE INFORMATION

File Name: installer3830.apk
Size: 2.37MB
MD5: f824594fb15ef2f5edbd0fbaf1ec1f7b
SHA1: 901f3cf54f1a1200352a10674f301159e7d2578f
SHA256: 5ab00f0d768c558471498ca2863fa0890cc45705c92abf66487068827ac5ecb4

ℹ APP INFORMATION

App Name: Checkers
Package Name: org.secuso.privacyfriendlydame
Main Activity: org.secuso.privacyfriendlydame.ui.SplashActivity
Target SDK: 28
Min SDK: 21
Max SDK:
Android Version Name: 1.2
Android Version Code: 3

🔲 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=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.

🔎 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/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/RequestManagerFra

NO	ISSUE	SEVERITY	STANDARDS	FILES
				gment.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/load/data/mediastore/Thumb Fetcher.java com/bumptech/glide/load/engine/bitmap_recycle/Lr uBitmapPool.java com/bumptech/glide/manager/DefaultConnectivity MonitorFactory.java com/bumptech/glide/load/resource/bitmap/VideoD ecoder.java com/bumptech/glide/load/engine/cache/DiskLruCac heWrapper.java com/bumptech/glide/load/engine/prefill/BitmapPre FillRunner.java com/bumptech/glide/load/resource/bitmap/Drawab leToBitmapConverter.java com/bumptech/glide/load/model/ByteBufferEncode r.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/Glide.java com/bumptech/glide/load/engine/executor/Runtime Compat.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/gifdecoder/GifHeaderParser.ja va com/bumptech/glide/manager/DefaultConnectivity Monitor.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/resource/gif/GifDrawable Encoder.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/gifdecoder/StandardGifDecod er.java com/bumptech/glide/load/model/ByteBufferFileLoa der.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.ja va com/bumptech/glide/load/resource/bitmap/Transfo rmationUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/util/pool/FactoryPools.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/request/target/CustomViewTarget.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/RequestManagerRetriever.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/EngineResource.java

🪪 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.

🔑 HARDCODED SECRETS

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.